TESIS DOCTORAL

LA FIGURA DEL RESPONSABLE EN EL DERECHO A LA PROTECCIÓN DE DATOS

Génesis y evolución normativa ante el cambio tecnológico y en perspectiva multinivel

Autora:
Ana Belén DURÁN CARDO

Directora de la tesis:
Dra. María Jesús GARCÍA MORALES

2015

Programa de doctorado en Derecho Público y Filosofía Jurídico-Política (RD 1393/2007)
Departamento de Ciencia Política y Derecho Público
Facultad de Derecho
Universitat Autònoma de Barcelona

A mi madre

ÍNDICE

CAPÍTULO II

LA CONSOLIDACIÓN DE LA FIGURA DEL RESPONSABLE EN LA NORMATIVA EUROPEA SOBRE PROTECCIÓN DE DATOS: LA CENTRALIDAD DEL CONCEPTO

CAPÍTULO III

LA RECEPCIÓN DEL CONCEPTO DE RESPONSABLE EN LAS LEGISLACIONES EUROPEAS NACIONALES DE PROTECCIÓN DE DATOS

PARTE II
EL RESPONSABLE COMO ELEMENTO CLAVE EN LA REGULACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS

CAPÍTULO IV
EL RESPONSABLE COMO CRITERIO DE DETERMINACIÓN DE LA LEGISLACIÓN APLICABLE

CAPÍTULO V
EL ESTATUTO DEL RESPONSABLE EN LA DIRECTIVA 95/46/CE Y EN LAS LEGISLACIONES NACIONALES EUROPEAS

CAPÍTULO VI
EL ESTATUTO DEL RESPONSABLE EN LA LEGISLACIÓN ESPAÑOLA

CAPÍTULO VII
EL RESPONSABLE Y LAS GARANTÍAS DEL DERECHO A LA PROTECCIÓN DE DATOS

CONCLUSIONES

INTRODUCCIÓN

El derecho a la protección de datos de carácter personal es un derecho complejo que no ha tenido una gestación sencilla. Su origen lo encontramos en la concepción del derecho a la privacidad estadounidense, de la mano de la premonitoria visión del juez Thomas M. Cooley y la plasmación doctrinal de este derecho, que efectuaron Samuel D. Warren y Louis D. Brandeis. Esta primera defensa, que constituyó el llamado "*right to be alone*", derecho a ser dejado en paz, respondió al uso de una tecnología: la fotografía instantánea utilizada por quien sería el primer sujeto agresor: la prensa.

En Estados Unidos también se formuló la *informational privacy* (que se atribuye a Alan F. Westin) como la capacidad que tienen los individuos de controlar la información, que sobre ellos mismos, se comunica a terceros, y donde se elaboró una primera norma que recogía una regulación del tratamiento informático de la información (la *Fair Credit Reporting Act*, de 26 de octubre de 1970). Sin embargo, será también en Estados Unidos donde asistamos a los principales ataques efectuados, tanto por el Estado, como por el sector empresarial, al derecho a la privacidad, propiciados por la defensa de otros valores fundamentales para esta potencia: la seguridad, la libertad de expresión y el capitalismo.

En el continente europeo el derecho a la vida privada contenido en el artículo 8.1 del Convenio de Roma, de 4 de noviembre de 1950, para la Protección de los Derechos Humanos y de las Libertades Fundamentales, será el germen del derecho a la protección de datos. La doctrina sobre autodeterminación informativa se recogió en la sentencia sobre el censo, de 15 de diciembre de 1983, del Tribunal Constitucional Federal Alemán. No obstante, su consideración como un derecho fundamental autónomo, inicialmente vacilante, ha cristalizado en Europa con su consagración en la Carta de derechos fundamentales de la Unión Europea. En España, con una premonitoria base jurídica ubicada en el artículo 18.4 de la Constitución española de 1978, el Tribunal Constitucional reconoció, en el año 2000, la autonomía de este derecho y su diferenciación del derecho a la intimidad, al que se había ligado inicialmente el mismo.

El nacimiento del derecho a la protección de datos respondió a una concepción generacional de los derechos que entendía que, estos, deben configurarse como un catálogo abierto a nuevas necesidades de protección[1]. La informática constituyó la aparición de una nueva forma de poder[2] ante la que los derechos a la intimidad o a la vida privada no otorgaban suficiente protección. Lo que se precisaba era proteger a las personas de la capacidad de acumular datos que proporcionaba la tecnología a unos sujetos que podían ostentar, en consecuencia, un poder sobre estos titulares de los datos. Datos, que por separado no podrían dañar a estas personas, sin embargo, si se unieran a otros, podrían comportar un perjuicio para las mismas. Se trataba, por tanto, de restablecer un equilibrio de fuerzas, entre los sujetos tratadores de datos y los sujetos cuyos datos eran tratados.

Con el fin de alcanzar ese equilibrio, la configuración del derecho a la protección de datos no se limitó a ser un derecho de defensa, como el derecho a la intimidad, sino que se caracterizó por ser un derecho proactivo. En palabras del Tribunal Constitucional "el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado" (STC 292/2000 de 30 de noviembre de 2000, FJ 6).

Estos aspectos se plasmaron en la normativa que desarrolló el derecho en el ámbito europeo, en las leyes nacionales que se promulgaron, así como en instrumentos internacionales, como el Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Posteriormente en la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que

[1] De esta forma, se insertaba en los denominados derechos de tercera generación, cuyo principal rasgo diferencial era la idea de solidaridad, de derechos que exigen para su realización la comunidad de esfuerzos y responsabilidades a nivel universal. A.E. PÉREZ LUÑO, *La tercera generación de derechos humanos*, Aranzadi, Cizur Menor (Navarra), 2006, págs. 34 a 36, 42.

[2] La informática constituye, para FROSINI, una tercera fase en la historia de la comunicación hablada del hombre. La primera fase ha sido la de la palabra oral, la segunda fase la de la palabra escrita y la tercera fase es la del lenguaje electrónico, que no es ni hablado ni escrito, sino un lenguaje totalmente artificial. La informática es una nueva forma de energía intelectual que constituye una nueva forma de poder, que puede ser concentrado o difundido en una sociedad, de forma que podrá ser un elemento cohesionador o un instrumento de sumisión. El autor estima que, sobre esta alternativa se juega el destino social del hombre. V. FROSINI, *Cibernética, derecho y sociedad*, Tecnos, Madrid, 1982, págs. 174 a 175.

respecta al tratamiento de datos personales y a la libre circulación de estos datos y las leyes nacionales que la transpusieron.

Pero, incluso este derecho moderno, nacido para protegernos de la utilización de la tecnología, se ha enfrentado a una evolución de la misma, difícilmente abarcable por la legislación que lo desarrolla. Los principios, recogidos en esta normativa, se establecieron en un momento en el que el uso de Internet era incipiente. Y es que desde la aparición, a finales de los años sesenta, de la informática, la evolución de la tecnología se ha precipitado.

Las nuevas generaciones, los "nativos digitales", han crecido y han aprendido a comunicarse a través de las redes sociales, los *blogs*, los vídeos e imágenes. Las herramientas y plataformas que permiten la interacción se descubren como infinitas en tendencias que, a medida que escribo estas palabras, quedarán desfasadas. Así se acuñan términos como computación en la nube (*cloud computing*), el Internet de las cosas *(Internet of things)* o el *big data,* en alusión al gran volumen de información volcado en Internet.

Esta nueva manera de comunicarnos nos obliga a exponer nuestros datos y somos nosotros mismos, quienes voluntariamente entregamos nuestra vida a otros. Estos datos que exponemos no se quedan en el limbo sino que alguien los posee. Los modelos de negocio surgidos de las posibilidades que brindan las tecnologías y, especialmente, Internet, ya no cobran dinero por los servicios de interacción que ofrecen, sino que se alimentan de esa información. Estos datos se han revelado como una mercancía valiosa que se puede analizar automáticamente para obtener informaciones que guíen a las empresas de forma más certera en las estrategias de venta de sus productos y servicios. Los datos, en definitiva, se han convertido en una materia prima.

No sólo eso, los Estados también se alimentan de estos datos que vuelcan de forma generosa sus titulares. Los objetivos que persiguen los Estados son diversos. Por un lado, el servicio público, de forma que también el Estado quiere aprovechar las bondades de las tecnologías para brindar mejores servicios a sus ciudadanos, de la mano de la administración electrónica. No obstante, la defensa de sus ciudadanos, acuciada por la amenaza terrorista, ha originado que se acuda a esta información en su nombre, con

resultados que se han revelado excesivos y no ajustados a lo que debería ser un Estado de derecho. La ciberinteligencia ha explotado esta información y se ha visto ayudada, tanto por el ingente volumen de la misma, como por las potentes herramientas que se han generado para analizarla.

Sector público y privado confluyen en el interés por los datos. Así sujetos, antaño contrapuestos, ahora se retroalimentan con esos datos, mediante nuevos instrumentos que se crean en nombre de la innovación, como la reutilización de los datos (conocido como *open data*) o, en nombre de la seguridad, como los accesos a sistemas de información privados por parte de autoridades (como sucede con los sistemas de videovigilancia).

Por ello, en el centro de la regulación del derecho a la protección de datos se encuentran las entidades públicas o privadas bajo la figura del responsable. Esta figura quiere representar al sujeto potencialmente agresor y responder a las preguntas: ¿ante quién debe luchar el derecho a la protección de datos?, ¿quién es el enemigo?, ¿el Estado?, ¿las empresas?, ¿nosotros mismos? Lo cierto es que las principales regulaciones mencionadas, como la Directiva 95/46/CE, nacieron con un objetivo principalmente económico, que lo que perseguía era garantizar que estos responsables pudieran tratar datos de carácter personal y hacerlos circular en el interior de un territorio, sin hallar trabas. Para ello, se quería uniformizar la protección que los Estados proporcionaban a sus ciudadanos en todo este territorio y, de esta forma, evitar que se favorecieran las empresas de un Estado, por encima de las de otro.

La figura del responsable, en estas regulaciones del derecho a la protección de datos de carácter personal, se erige como una pieza fundamental. Su existencia se justifica por la necesidad de establecer, un sujeto obligado a cumplir con las obligaciones establecidas en la legislación que regula este derecho y, como consecuencia, a responder de los posibles incumplimientos. La determinación de los sujetos obligados dibuja el ámbito de aplicación de estas normativas y, en la Directiva 95/46/CE y su normativa de transposición, constituye también uno de los criterios para solucionar conflictos sobre la legislación aplicable.

Este trabajo persigue profundizar en el conocimiento de esta figura, desde su origen en las primeras leyes nacionales europeas de los años setenta, hasta su presente en

las diversas normativas europeas e internacionales y su futuro en las reformas apuntadas. En este camino a recorrer se dirigirá la atención a los factores que hacen de esta figura un eje del derecho a la protección de datos.

No obstante, la premisa de la inserción de la figura en la regulación es conseguir identificar al sujeto agresor, para lo que se acude a la fórmula de la definición. Así, la diferenciación de la figura en estas regulaciones se ha plasmado en el uso de un concepto que se diseccionará con el fin de mostrar sus elementos. De esta forma, se quiere presentar una metodología que ayude a la identificación del responsable y que encuentra su fundamento en un dictamen del Grupo del Artículo 29 (formado por representantes de las autoridades de control de protección de datos europeas)[3] y en la única obra monográfica dedicada al responsable, desde la perspectiva de la responsabilidad civil, que llevó a cabo Pedro Grimalt Servera[4].

Llama la atención que este sujeto central en el derecho de protección de datos no haya merecido apenas atención doctrinal hasta ahora. Por el contrario, sí se ha analizado la figura del delegado de protección de datos o encargado independiente que, pese a ser también un sujeto importante, carece de la centralidad del responsable[5]. No obstante, existen menciones al responsable, en el ámbito de obras generales dedicadas al derecho, pero no hay trabajos que lo traten de forma integral. Hay que destacar el trabajo realizado por Antonio Troncoso Reigada, que analiza la determinación del responsable, especialmente en el ámbito de las administraciones públicas[6]. Emilio Del Peso Navarro es uno de los autores que se acercó a la figura del responsable, en sus análisis sobre la normativa y que señaló la necesidad de que se estudiara con profundidad, al considerarla uno de los ejes sobre los que el legislador hacía girar la protección de los datos de

[3] Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", 00264/10/ES WP 169, 16.2.2010, Grupo de trabajo Artículo 29 sobre la protección de datos.
[4] P. GRIMALT SERVERA, *La responsabilidad civil en el tratamiento automatizado de datos personales*, Comares, Granada, 1999.
[5] F.J. SANTAMARÍA RAMOS, *El encargado independiente. Figura clave para un nuevo derecho de protección de datos*, La Ley, Las Rozas (Madrid), 2011.
[6] Especialmente ver A. TRONCOSO REIGADA, *La protección de datos personales. En busca del equilibrio*, Tirant lo Blanch, Valencia, 2010.

carácter personal[7]. Este autor, junto a Miguel Ángel Ramos González, aludió a los problemas que daría su aplicación[8].

La idea de abordar la figura del responsable surge precisamente de los problemas que encontré yo misma en su determinación, en la aplicación práctica de la regulación del derecho. Desde que inicié mi andadura profesional, como abogada especializada en el derecho a la protección de datos, en el año 2000, con la aprobación de la ley vigente española en esta materia, he comprobado las dificultades en la aplicación del concepto. Eché de menos, en ese momento, algún trabajo que ofreciera criterios, una metodología que me ayudara a realizar el análisis jurídico de determinación del responsable. He querido, por lo tanto, realizar un trabajo que llenara ese vacío y que analizara, no sólo desde el punto de vista teórico, sino sobre todo, desde el punto de vista práctico, al responsable.

He intentado responder a las cuestiones que me planteaba la figura. Así, ante el análisis de un supuesto de hecho, la identificación del responsable es un *prius* necesario para la aplicación de la legislación, por lo que es imprescindible responder a las preguntas: ¿quién es el responsable? ¿Cómo determinarlo? ¿Cuáles son los elementos que permiten su identificación? ¿Cómo diferenciarlo de otras figuras como el encargado del tratamiento? ¿Cómo saber cuándo se aplica la legislación en función de los criterios que toman como referencia el establecimiento del responsable? Y una vez determinado: ¿qué obligaciones debe cumplir? ¿Tiene derechos el responsable? ¿Cómo se integra en el marco de garantías del derecho?

Inicié este trabajo a principios del año 2012, en el momento en el que la Comisión Europea presentó el paquete de reforma de la normativa europea sobre el derecho a la protección de datos. Paralelamente, también está en proceso de reforma el Convenio nº 108 del Consejo de Europa. Nos hallamos, por tanto, en un punto de inflexión.

[7] E. DEL PESO NAVARRO, "La figura del responsable del fichero de datos de carácter personal en la LORTAD", *Informática y derecho: Revista iberoamericana de derecho informático*, Nº 6 a 7, 1994, págs. 252, 258, 267.
[8] E. DEL PESO NAVARRO, M.A. RAMOS GONZÁLEZ, *Lortad: análisis de la ley*, Díaz de Santos, Madrid, 1998, pág.106.

La reforma de la Directiva 95/46/CE lo cambiará todo en este ámbito, ya que se sustituirá por un reglamento europeo que desplazará, por lo tanto, la normativa nacional vigente en los Estados miembros. El objetivo es lograr, esta vez, un nivel mayor de armonización. La importancia de esta modificación ha implicado que el procedimiento legislativo emprendido se alargue en virtud de los importantes intereses económicos, jurídicos y políticos que se han planteado. Muestra de ello, ha sido el *lobby* sin precedentes por parte de gobiernos y grandes empresas tecnológicas quienes, ante una normativa más estricta, ven peligrar su acceso a la materia prima que alimenta sus negocios.

Esta propuesta de reforma, junto a la carencia de trabajos que se aproximaran a la figura y la estrecha conexión del derecho de protección de datos al contexto social, económico y político, son elementos que han influido en el enfoque metodológico de este trabajo. Pero además, en un entorno global como en el que vivimos, no sólo se puede tener en cuenta la legislación nacional, ni siquiera la europea, sino que también hay que mirar hacia los instrumentos internacionales, de forma que hay que abarcar el ámbito multinivel de protección de los derechos. Esto se acentúa en un derecho vinculado especialmente al uso de una herramienta tecnológica de alcance mundial, como es Internet.

Como consecuencia de estos aspectos, ha sido necesario aproximarse, no sólo a la doctrina existente sobre el derecho a la protección de datos, sino también directamente a un gran número de documentos normativos y no normativos de ámbito estatal, autonómico, europeo e internacional. El análisis se ha efectuado en dos planos, uno más teórico relativo a la normativa, a su proceso de elaboración y a su contenido; otro referido a la aplicación práctica de esta normativa.

En este sentido, hay que resaltar que todo aquel que se aproxima al derecho de protección de datos, sabe que resulta fundamental examinar la abundante documentación que generan las autoridades de control y, en especial, el Grupo del Artículo 29, ya mencionado. Las autoridades proporcionan, mediante esta documentación, sus criterios a la hora de aplicar la normativa. Asimismo, es necesario, para tener en cuenta esta aplicación práctica, el estudio de la jurisprudencia emanada por las diferentes jurisdicciones competentes.

Debido a la inminente reforma, se incidirá especialmente en el análisis de la Directiva 95/46/CE, ya que conformará el antecedente futuro del reglamento europeo que se apruebe, así como en la jurisprudencia del Tribunal de Justicia de la Unión Europea. Y sin embargo, tampoco se ha querido dejar de lado el estudio del derecho comparado, de forma que se han incluido en el ámbito del estudio las leyes de protección de datos de los Estados miembros, no sólo de la Unión Europea, sino de los que integran el Espacio Económico Europeo, que también aplican la Directiva 95/46/CE.

Evidentemente, se ha profundizado en el ordenamiento español, ya no sólo porque es el que nos afecta más de cerca, sino porque posee una de las regulaciones más singulares de la figura del responsable.

Asimismo, se han incluido en el trabajo normas de otros países y organizaciones internacionales, especialmente importantes por su aplicación o influencia en el derecho de protección de datos europeo, como son las de Estados Unidos, el Consejo de Europa, la Organización de Naciones Unidas, la Organización de Cooperación y Desarrollo Económico y el foro de Cooperación Asia-Pacífico. También se han querido incluir referencias a instrumentos o elaboraciones jurídicas de gran interés, como la Propuesta conjunta para la redacción de estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal, adoptada en Madrid, en 2009, o proyectos como el de *accountability* que lleva a cabo *The Centre for Information Policy Leadership Hunton&Williams LLP*.

Toda esta aproximación jurídica se realiza en conexión con el contexto histórico en el que se desarrollaron las normas estudiadas.

Así, la primera parte de este trabajo se centra en el estudio del concepto de responsable, de forma que se identificará el momento histórico en el que se originó el mismo en el derecho positivo europeo. Otro objetivo será identificar y analizar los diversos elementos que conforman este concepto de responsable en las diversas leyes donde aparece para construir una metodología que facilite su determinación. Al mismo tiempo que se define al responsable, se delimitará mediante su contraposición con la figura del encargado del tratamiento.

La segunda parte de la tesis recoge los factores que hacen del responsable una figura clave en la normativa europea de protección de datos. En primer lugar, se abordará cómo el responsable es protagonista en el establecimiento de los criterios de resolución de conflictos sobre la legislación aplicable. En segundo lugar, nos aproximaremos al estatuto del responsable, ya que la principal misión del responsable será cumplir con las obligaciones que derivan de la normativa que regula el derecho a la protección de datos. Finalmente, el responsable jugará un papel importante en el sistema de garantías previsto para proteger el derecho de protección de datos. Para analizar este papel, se recorrerán los principales mecanismos previstos por este sistema: el ejercicio de derechos, los mecanismos procesales, la responsabilidad civil, penal y el régimen sancionador.

En la tercera parte de la tesis se quiere mostrar cómo la figura del responsable se enfrenta a los retos creados por el desarrollo tecnológico en la actualidad y los avances en las reformas que se llevan a cabo en torno a la regulación del responsable. De esta forma, se ofrecerá una panorámica de las vicisitudes a las que se enfrenta la regulación del responsable ante las tensiones originadas por una normativa que se creó cuando el uso de Internet era incipiente y las soluciones que se han adoptado por autoridades y tribunales, encargados de suplir esta inadaptación. El futuro inminente del responsable se plasma en los textos que conforman el proceso de reforma de la Directiva 95/46/CE. Se extraerán de los mismos las novedades para esta figura, como la adopción de un nuevo enfoque de autorresponsabilidad. Todo ello sin olvidar la modernización del Convenio 108 y un proyecto de ley, presentado en el Congreso estadounidense: la *Consumer Privacy Bill of Rights Act.*

En definitiva, con esta tesis pretendo llenar un vacío bibliográfico y ayudar a aquéllos, que como yo misma, se dedican a este apasionante mundo de la protección de datos, ya sea desde el mundo académico o desde el mundo del ejercicio de la abogacía. De esta forma, además de un riguroso trabajo académico, que profundiza en la figura desde un punto de vista jurídico, pretendo ayudar con él a quienes se enfrentan al análisis de supuestos de hecho, que requieren de una decisión sobre la estrategia jurídica a seguir en el cumplimiento de la legislación de protección de datos y en la que el primer paso es saber si el sujeto analizado es o no es responsable del tratamiento.

Durante el transcurso de los años que he dedicado a este apasionante proyecto muchas son las personas con las que he podido contar y que me han dado apoyo. No puedo dejar de plasmar en estas líneas mi agradecimiento a todas ellas.

En primer lugar quiero agradecerle a mi directora de tesis, la Dra. María Jesús García Morales, por ser la persona que me animó a iniciar este viaje, pero, especialmente, a quien, sin duda, debo el haber podido llegar hasta el final. Su apoyo incondicional, su profesionalidad, su guía, su compromiso y, sobre todo, su amistad, forman parte de cada una de estas páginas. También quiero darle las gracias a mi socia y amiga Cristina Serrano Sánchez, con quien conocí este apasionante mundo de la protección de datos y que ha estado ahí para ayudarme a compaginar este proyecto con mi trabajo, algo, en ocasiones, bastante complicado. También tengo que agradecerle nuestros numerosos debates y sus innumerables preguntas, que, sin duda, han hecho mi trabajo mejor.

Quiero agradecer al Dr. Joan Manel Abril Campoy, catedrático acreditado de Derecho Civil y Magistrado del Tribunal Superior de Justicia de Cataluña, por su generosidad, al haber aceptado leer el capítulo dedicado a la responsabilidad, y ofrecerme sus valiosos comentarios y apreciaciones que espero haber merecido.

En la fase final de redacción de esta tesis, la Agencia Española de Protección de Datos, me brindó la oportunidad de llevar a cabo una estancia de investigación, durante la que pude entrevistar a responsables de las áreas de Internacional, Registro y Gabinete jurídico y consultar el fondo bibliográfico de esta institución. Quiero poner de relieve la filosofía de apertura y de fomento del conocimiento que siempre ha protagonizado la Agencia. Sin duda, este espíritu hace más fácil que se profundice en este derecho tan complejo y que se ha mostrado esencial en esta era digital en la que vivimos.

Fue especialmente enriquecedora la estancia y no quiero dejar pasar la ocasión de agradecer a todas y cada una de las personas que me hicieron sentir como en casa y que dedicaron una gran parte de su tiempo a esta investigación. Quiero agradecer a María José Blanco Antón, Secretaria General de la AEPD por autorizar mi estancia, y a María José González Estévez, Jefa de Servicio de Secretaría General y Natalia Pazos Gómez, Jefa de Negociado de Secretaría General, por hacer posible esta experiencia, organizar las entrevistas y asistirme en todo momento.

Por último, dar las gracias por la generosidad, tanto en el tiempo que me brindaron en las entrevistas, como en sus interesantes aportaciones a: Rafael García Gozalo, Vocal Asesor Jefe del Área Internacional; Lourdes Hernández Crespo, Jefa de Servicio de la Unidad de Apoyo a la Dirección; Julián Prieto Hergueta, Subdirector General del Registro General de Protección de Datos; Manuel Villaseca López , Jefe de Área del Registro General de Protección de Datos y Manuel García Sánchez, Jefe de Servicio del Área Internacional.

Asimismo, quiero agradecer a todos los bibliotecarios que me han ayudado en las bibliotecas que he tenido ocasión de consultar: la del Consell de Garanties Estatutàries de la Generalitat de Catalunya, la del Il·lustre Col·legi d'Advocats de Barcelona, la de la Universitat Autònoma de Barcelona y la de la Universidad de Barcelona. Todas esas personas las quiero individualizar en Maria Teresa Massas, de la biblioteca del Consell de Garanties Estatutàries, que ha hecho que mi labor de investigación haya sido, sin duda, más fácil. Espero, que pese a todos los avances tecnológicos, nunca desaparezcan, ni ellos ni las bibliotecas.

Por último, quiero agradecer también a mi familia y a mis amigos, simplemente, por estar allí, cuando yo no estaba.

ABREVIATURAS

ACPD: *Autoritat Catalana de Protecció de Dades*

AELC: Asociación Europea de Libre Cambio o Acuerdo Europeo de Libre Comercio

AEPD: Agencia Española de Protección de Datos

APEC: *Asia-Pacific Economic Cooperation*

APEC Privacy Framework*: Asia-Pacific Economic Cooperation Privacy Framework*

Carta UE: Carta de Derechos Fundamentales de la Unión Europea

Cc: Código Civil

Comisión: Comisión Europea

Consejo UE: Consejo de la Unión Europea

CEDH: Convenio de Roma, de 4 de noviembre de 1950, para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

Convenio 108: Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

CPBR: *Consumer Privacy Bill of Rights*, incluida en *Consumer data privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy*.

CPBRA: *Consumer Privacy Bill of Rights Act of 2015*.

Decisión Marco 2008/977/JAI: Decisión Marco 2008/977/JAI del Consejo de 27 de noviembre de 2008 relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.

Decisión *Safe Harbour*: Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE de Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.

Directiva 95/46/CE: Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Directiva 2000/31/CE: Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

Directiva 2002/58/CE: Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

EEE: Espacio Económico Europeo

EEUU: Estados Unidos

FIIPs: *Fair Information Practice Principles*

FRA: Agencia de Derechos Fundamentales de la Unión Europea

GA29: Grupo de protección de las personas en lo que respecta al tratamiento de datos personales o Grupo del Artículo 29.

Guía OCDE 1980: Guía de la OCDE relativa a la protección de la privacidad y de las transferencias de datos personales aprobada por resolución del Consejo de 23 de septiembre de 1980.

Guía OCDE 2013: *Recommendation of the Council concerning Guidelines governing the protection of privacy and transborder flows of personal data (2013), C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79.*

Ley canadiense: *Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c. 5

Ley catalana: Ley 32/2010, de 1 de octubre, de la Autoritat Catalana de Protecció de Dades.

Ley mexicana: Ley federal de protección de datos personales en posesión de los particulares, 5.07.2010.

Ley vasca: Ley 2/2004, de 25 de febrero de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos

LO 1/1982: Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

LORTAD: Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

LSSI: Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

OCDE: Organización de Cooperación y Desarrollo Económico

PCE-Directiva policía: Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.

PCE-RGPD: Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), 25.1.2012.

PCE-RGPD no oficial: *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), draft, Version 56 29.11.2011*.

PCJ-RGPD: Nota de la Presidencia al Consejo sobre Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)-Preparación de un planteamiento general, Expediente interinstitucional: 2012/2011 (COD) 9565/15, Bruselas, 11.6.2015.

PE: Parlamento Europeo

PPE-Directiva policía: Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos.

PPE-RGPD: Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos).

Principios rectores ONU: Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales aprobados por la Resolución 45/95 de la Asamblea General de Naciones Unidas, de 14 de diciembre de 1990.

Propuesta de Directiva de 1990: Propuesta de Directiva del Consejo relativa a la protección de las personas en lo referente al tratamiento de datos personales, COM(90) 314 final, DO C 277 de 5.11.1990, pág. 3.

Propuesta de Directiva de 1992: Propuesta modificada de Directiva del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, COM (92) 422 final, DO C 311 de 27.11.1992, pág. 30.

Propuesta de Madrid: Propuesta conjunta para la redacción de estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal, adoptada en Madrid en 2009.

Proyecto sobre accountability: proyecto sobre *accountability* que lleva a cabo *The Centre for Information Policy Leadership Hunton&Williams LLP*.

Reforma C108: *Abridged report of the 3rd and final meeting (Strasbourg, 1-3 December 2014), CM(2015)40, Ad hoc Committe on Data Protection (CAHDATA), Council of Europe, Strasbourg, 3 March 2015*.

Reglamento 45/2001: Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo de 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

Reglamento de desarrollo de la Ley mexicana: Reglamento de la ley federal de protección de datos personales en posesión de los particulares, 21.12.2011.

RLOPD: Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

TC: Tribunal Constitucional

TEDH: Tribunal Europeo de Derechos Humanos

TJUE: Tribunal de Justicia de la Unión Europea

TFUE: Tratado de Funcionamiento de la Unión Europea

TUE: Tratado de la Unión Europea

UE: Unión Europea

PARTE I
EL ORIGEN Y LA CONSOLIDACIÓN DEL CONCEPTO DEL RESPONSABLE EN EL DERECHO EUROPEO

En la primera parte de este trabajo se quiere ofrecer un análisis del concepto de responsable. Como somos el reflejo de nuestro pasado, es necesario acudir al origen y atender también al camino que ha seguido la figura del responsable hasta llegar a la regulación actual. Se inicia esta andadura en Estados Unidos (EEUU), aunque deberemos acudir al continente europeo, para descubrir el origen del concepto de responsable y su consolidación en la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Directiva 95/46/CE).

CAPÍTULO I
EL ORIGEN DEL RESPONSABLE, UN INSTITUTO DEL DERECHO EUROPEO

En el presente capítulo se analizará el origen del concepto de responsable. Este concepto, inexistente en la génesis del derecho a la privacidad que se encuentra en el derecho anglosajón y en el Convenio de Roma, de 4 de noviembre de 1950, para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH), se abre camino en las primeras leyes europeas que datan de los años setenta. A raíz de las mismas, se incorpora el concepto en los primeros instrumentos internacionales que regularon el derecho a la protección de datos. El más importante de estos instrumentos es el Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108) que, pese a introducir el concepto, no lo incorporará en el cuerpo de su regulación. Tendrá que esperar, por tanto, el concepto, para poder adquirir el protagonismo que le brindará su incorporación de pleno en una regulación.

1. LA AUSENCIA DE LA CATEGORÍA DE RESPONSABLE EN LA GÉNESIS DEL DERECHO A LA PRIVACIDAD

En la época de los griegos y los romanos una persona no era nada sino participaba de la vida pública, lo que no casaba con la concepción de la intimidad. En la sociedad actual se podría hacer un paralelismo con esa otra época y pensar que una persona no es nada si al teclear su nombre en un buscador, no aparece información de ella en Internet[9].

En EEUU se verá que la regulación de la privacidad, a nivel federal, no ha establecido una categoría formal de responsable asimilable a la que se incorporará en la normativa europea. Los motivos son, primero, porque el principal sujeto obligado a respetar este derecho es el Estado, por lo que se entiende que es más fácilmente definible. Un segundo motivo es porque, en este país, se ha optado por establecer un sistema de protección de la privacidad consistente en leyes federales sectoriales, destinadas al sector privado, sólo para determinados colectivos de sujetos obligados. Al ser colectivos concretos no requieren de mayor determinación o encasillamiento, pues su sujeción a la norma viene establecida por el desarrollo de una actividad económica y/o empresarial.

Pese a que en EEUU no existe la figura del responsable, es importante prestar atención a su regulación, ya que, como se verá más adelante, tendrá gran influencia en las normas que se preparan en Europa para regular el derecho a la protección de datos. Igualmente es importante prestar atención a este país, ya que aquí nacen la informática e Internet, fenómenos clave en el surgimiento y en la progresiva relevancia del derecho a la protección de datos.

[9] SOLOVE y SCHWARTZ denominan a este fenómeno la *Googleization*. La información sobre cualquier persona se encuentra fácilmente, al "*Google*ar" su nombre. D.J. SOLOVE, P.M. SCHWARTZ, *Information Privacy Law*, 4ª ed., Wolters Kluwer Law & Business, New York, USA, 2011, págs. 8 a 9.

1.1. La inexistencia del concepto en el sistema anglosajón, cuna del derecho a la privacidad

1.1.1. La formulación del derecho a la privacidad ante la insuficiente protección del Common Law

El derecho a la protección de datos o derecho a la autodeterminación informativa nace ligado al derecho a la intimidad, derecho que a su vez halla su antecedente en la libertad individual propia del liberalismo[10]. En el modelo clásico de sociedad la idea de libertad se reflejaba en la participación en la vida política, pero con una completa

[10] Hay que decir que entorno al derecho a la protección de datos ha habido una gran confusión terminológica debido a su tardío reconocimiento como derecho autónomo. Esto produjo que se tuviera que fundamentar en otros derechos como el de la intimidad en España o el derecho a la vida privada en el marco del CEDH, como se verá. Como resultado, actualmente el derecho recibe multitud de denominaciones que no siempre son equiparables. Es lo que REMOLINA ANGARITA ha denominado pluralismo terminológico. N. REMOLINA ANGARITA, *Recolección internacional de datos personales: un reto del mundo post-Internet, Premio protección de datos personales de investigación 2014 Iberoamérica*, Agencia Española de Protección de Datos, Agencia Estatal BOE, Madrid, 2015, págs. 95 a 97. En EEUU se habla de derecho a la *privacy* o a la privacidad, lo que no debe llevarnos a equiparar este derecho con el de intimidad, ni tampoco con el derecho a la protección de datos europeo, ya que el derecho a la privacidad englobaría a ambos. La confusión terminológica existente alrededor de este derecho se ilustra en nuestro ordenamiento mediante la jurisprudencia del TC, en la que incluso cuando se inició el reconocimiento del derecho a la protección de datos como derecho autónomo, se aludía al mismo tiempo al derecho a la intimidad. Además, inicialmente, el TC también aludió a este derecho como "libertad informática" o *habeas data*. Así, por ejemplo, en la STC 254/1993, FJ 7 indica "la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data)". No se aclaró la diferenciación hasta la STC 292/2000 que sienta la doctrina constitucional sobre el derecho a la protección de datos. A esta terminología cabe añadir el término privacidad que se incluyó en la exposición de motivos de la LORTAD y mediante el que el legislador quiso aclarar que el derecho protegido iba más allá del derecho a la intimidad. Hay también doctrina que ha considerado que este derecho a la protección de datos se define mejor con la denominación de derecho a la autodeterminación informativa, ya que más que ligarlo al artículo 18.4 CE se enlaza con el artículo 10.1 CE que reconoce la dignidad de la persona. I.C. DEL CASTILLO VÁZQUEZ, *Protección de datos: cuestiones constitucionales y administrativas. El derecho a saber y la obligación de callar*, Civitas, Madrid, 2007, pág. 138. Respecto a esta cuestión hay que citar el Voto particular que formuló el Magistrado don Manuel Jiménez de Parga y Cabrera a la STC 290/2000, al que se adhirió el Magistrado don Rafael de Mendizábal Allende. En el mismo defendieron que la libertad informática era un derecho de los considerados no escritos en la Constitución y debía tener como eje vertebrador el artículo 10.1 CE, al ser un derecho inherente a la dignidad de la persona, de forma que no debía incardinarse en el artículo 18.4 CE. Ambos Magistrados entendieron que los principios que establece el artículo 10.1 CE son principios constitucionales, por lo que todo el ordenamiento debe interpretarse conforme a los mismos y además son principios directamente vinculantes (apdos. 3 y 4). En todo caso, estimo que el derecho a la protección de datos ya ha sido plenamente reconocido y lo adecuado es hacer referencia al mismo con esta denominación. No obstante, dado que existe esta confusión muchos de los instrumentos, incluso los europeos alimentan la misma, por lo que me veré obligada a referirme en algunos casos a otros términos.

sumisión a la autoridad en la que no cabía el derecho a la intimidad. A este modelo clásico se contrapone el modelo liberal, en el que se quiere primar el individualismo[11].

Los autores señalan diversas aportaciones como antecedentes de la protección de la privacidad. En este sentido, se identifica la máxima recibida en el derecho colonial procedente de la tradición jurídica inglesa que entendía la casa de cada uno como su castillo ("*a man's house as his castle*") y que reivindicaba la protección del individuo en su hogar[12]. Esta máxima fue incorporada por las colonias norteamericanas y alcanzó reconocimiento constitucional en 1791, en la Tercera Enmienda de la Constitución de EEUU, que prohíbe la requisa de domicilios particulares por los soldados sin el consentimiento de sus propietarios en tiempos de paz; en la Cuarta Enmienda que protege de registros arbitrarios (*unreasonable searches and seizures*) y en la Quinta Enmienda que protege frente a la incriminación contra uno mismo e impide que el gobierno le obligue a revelar información personal y reservada[13].

El juez Thomas M. Cooley analizó estas enmiendas junto a la máxima "*a man's house as his castle*" en *A Treatise on the Constitutional Limitations which Rest upon the Legislative Power of the States of the American Union* (1868) y afirmó que contribuían a la protección de la privacidad del individuo[14]. En 1879, el mismo Cooley, aludió a la expresión "*the right to be let alone*" o derecho a ser dejado en paz en la primera edición

[11] BENJAMIN CONSTANT contraponía la libertad de los antiguos que se manifestaba en la esfera de lo público a la libertad de los modernos que consiste en el disfrute de la vida privada. De esta forma, alertaba que, mientras el peligro de la libertad antigua era que los hombres, atentos únicamente a asegurarse la participación en la vida social, despreciaran los placeres individuales, el peligro de la libertad moderna era que, absorbidos por la búsqueda de los intereses particulares, los hombres renunciaran al derecho de participación en el poder político. B. CONSTANT, "De la libertad de los antiguos comparada con la de los modernos", *Escritos Políticos* (Estudio preliminar, traducción y notas de María Luisa Sánchez Mejía), Centro de Estudios Constitucionales, Madrid, 1989, págs. 259 a 261, 282 a 283. Asimismo, WACKS recuerda que para los griegos el vivir apartado (*idion*) era por definición considerado *idiotic*, R. WACKS, *Personal Information, privacy and the law, Clarendon Press*, Oxford, 1989, pág.7.

[12] Se ilustra este principio en el discurso que pronunciara William Pitt ante el Parlamento inglés en 1763: "El hombre más pobre, en su cabaña, desafía todas las fuerzas de la Corona. [Su cabaña] puede ser frágil, su techo tal vez es inestable, el viento se cuela por él, la tempestad lo penetra, no impide el paso de la lluvia, pero el Rey de Inglaterra no puede entrar en ella; ni con todo su poder se atreve a cruzar el umbral de esa ruinosa morada". W. PITT, "Speech on the Excise Bill", en HANSARD, T.C. (ed.) (1753 a 1765). *The Parliamentary History of England from the Earliest Period to the Year* 1803, 23 vols., London, vol. 15, 1806 a 1820, pág. 1307, citado por M. NIEVES SALDAÑA, "The right to privacy. La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis", *Revista de Derecho Político* (UNED), núm. 85 2012, pág. 204.

[13] *Ibídem*, págs. 204 a 205.

[14] *Ibídem*, pág. 205.

de su *Treatise on the Law of Torts*[15]. En su análisis de la Cuarta y Quinta Enmiendas el juez afirmaba el derecho de la persona a protegerse frente a invasiones de la privacidad provocadas, tanto por las intromisiones ilegales de los agentes del gobierno, como por la curiosidad lasciva del público en general. En 1886, el Tribunal Supremo de EEUU trasladó estos argumentos al asunto *Boyd v. United States* y consideró que la obtención de documentos privados y su utilización como prueba iban en contra de la Cuarta y Quinta Enmiendas, al vulnerar el derecho a la libertad, a la seguridad personal y a la propiedad privada[16].

Sin embargo, es el conocido artículo de los abogados Samuel D. Warren y Louis D. Brandeis "*The Right to Privacy*", publicado en la *Harvard Law Review* en 1890[17], en el que no olvidan mencionar al juez Cooley[18], el que supone la formulación doctrinal y la asunción de la existencia del derecho a la privacidad en EEUU[19]. El desencadenante de este trabajo fue la reciente aparición, en aquella época, de la fotografía instantánea y su utilización por la prensa de la época[20]. Sin duda, el artículo mantiene total vigencia en el siglo XXI. Primero, en lo que se refiere a la constante lucha entre la libertad de

[15] T.M. COOLEY, *A Treatise on the Law of Tort or the Wrongs Which Arise Independently of Contract*, Chicago, Callaghan, que menciona M. NIEVES SALDAÑA, "The right to privacy. La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis", *op. cit.*, pág. 206. También aluden a esta aportación de T.M. COOLEY diversos autores como J. L. PIÑAR MAÑAS "Protección de datos: origen, situación actual y retos de futuro", P. LUCAS MURILLO DE LA CUEVA, J.L. PIÑAR MAÑAS, *El derecho a la autodeterminación informativa*, Fundación coloquio jurídico europeo, Madrid, 2009, pág. 82, en nota al pie 2, que se refiere a este texto pero a su segunda edición de 1888 y antes el mismo P. LUCAS MURILLO DE LA CUEVA, en *El derecho a la autodeterminación informativa (La protección de los datos personales frente al uso de la informática)*, Tecnos, Madrid, 1990, pág. 59, cita 32, pero que alude a la 4ª edición del texto de 1932.

[16] M. NIEVES SALDAÑA, "The right to privacy. La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis", *op.cit*, págs. 206 a 207.

[17] S.D. WARREN, L.D. BRANDEIS "The Right to Privacy", *Harvard Law Review*, Vol. 4 nº5 (Dic.15 1890), págs. 193 a 220.

[18] S.D. WARREN, L.D. BRANDEIS "The Right to Privacy", *op.cit.*, pág. 195.

[19] Según SOLOVE y SCHWARTZ este artículo es el más importante en materia de privacidad. D.J. SOLOVE, P.M. SCHWARTZ, *Information Privacy Law*, *op.cit.*, pág. 10.

[20] De hecho, algunos autores atribuyen la elaboración del artículo al acoso de la prensa de Boston al que se vio sometido uno de los dos abogados, Samuel L. Warren, por su matrimonio con la hija de un senador. Así lo explican A. R. MILLER, *The Assault on Privacy*, The University of Michigan Press, EEUU, 1971, pág. 170; R. MARTÍNEZ MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa*, Editorial Civitas, Madrid, 2004, págs. 66 a 67, en nota al pie 15. No obstante, NIEVES SALDAÑA indica que el nombre de Warren sólo se menciona en dos ocasiones en *The Saturday Evening Gazette* entre 1883 y 1890, por lo que no parecen probables estas tesis. Sin embargo, sí parece claro que Warren estaba molesto por los abusos de la prensa, lo que se deduce del intercambio de correspondencia entre él y Brandeis, siendo éste el que le sugiere la elaboración del artículo. M. NIEVES SALDAÑA, "The right to privacy. La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis", *op.cit*, págs. 209 a 210. SOLOVE y SCHWARTZ también apuntan como posible causa del artículo, la influencia de otro artículo escrito en 1890 por E.L. GODKIN, "The rights of the citizen to his own reputation", *Scribner's Mag*, 1890. D.J. SOLOVE, P.M. SCHWARTZ, *Information Privacy Law*, *op.cit.*, pág.10.

información y la protección de la intimidad. Pero, también, en cuanto se trata de una reflexión ante la aparición de una tecnología que facilita la agresión al derecho, de forma que, si en aquella época se trataba de la fotografía instantánea, actualmente podemos apuntar a la aparición de la informática, Internet y todas las nuevas tecnologías que permiten la recopilación, difusión y almacenamiento de información, antes impensables.

Warren y Brandeis constataron que los mecanismos de protección que se habían estado utilizando hasta ese momento, tanto en la legislación como en el *Common law*, para proteger la no publicación de informaciones referentes a los individuos, ya no eran suficientes. La ley contra el libelo y la difamación exigía que se produjera una lesión a la reputación de la persona, lo que no siempre sucedía si la información o las imágenes que se publicaban no producían esta lesión. Tampoco la protección de la propiedad era suficiente, ni la referida a la propiedad en general ni la referida a la propiedad intelectual en especial. Por último, tampoco se podía fundamentar siempre la publicación de informaciones privadas en la violación de una relación de confianza o contractual porque no siempre se iba a producir esta relación entre el que difunde la información y el individuo que es víctima de la difusión[21]. Lo que quería evitarse era que se publicaran informaciones o fotografías sobre la vida privada de las personas y así impedir que la vida privada se convirtiera en una mercancía para vender más periódicos[22].

[21] Según indican los autores, en algunos casos, los juzgados habían presentado como argumento para evitar la publicación de información la violación de una relación contractual implícita o de una relación de confianza. Como ejemplo mencionaban un asunto judicial, *Abernethy v. Hutchinson, 3 L.J. Ch. 209 (1825)*, en el que los asistentes a unas ponencias publicaban el contenido de las mismas. Se consideró que se trataba de una violación de la relación de confianza ya que la ponencia era oral y se entendía que su objetivo era la formación de los asistentes y no que estos sacaran provecho de la misma. En el asunto *Tuck v. Priester, 19 Q. B. D. 639 (1887)* referido al encargo de copias de un cuadro, en el marco del que el copista hizo un mayor número de copias que vendió, se consideró que constituía una violación de contrato. Existió violación de confianza en un asunto, *Pollard v. Photographic Co., 40 Ch. Div. 345 (1888)*, donde un fotógrafo hizo un retrato y luego lo vendió contraviniendo la prohibición de la retratada. WARREN y BRANDEIS concluyeron que el hecho de fundamentar la protección en la violación de contrato o de confianza funcionaba si los abusos eran poco frecuentes pero no era suficiente con la aparición de los modernos aparatos que otorgaban múltiples oportunidades de ocasionar estas vulneraciones sin que tuviera ocasión de intervención la persona afectada ni existiera relación contractual ni de confianza a la que acogerse. Así antes la fotografía exigía la pose y, por lo tanto, sí podía aplicarse la violación de confianza o de relación contractual, pero con la fotografía instantánea el fotografiado podía no ser consciente de que le fotografiaban y, por lo tanto, no podría generarse esta violación, al no tener la oportunidad esta persona de prohibir la divulgación. S.D. WARREN, L.D. BRANDEIS "The Right to Privacy", *op.cit.*, págs. 207 a 212.

[22] Actualmente, nos hallamos ante un dilema equivalente. Internet permite que los periódicos y cualquier persona, a través de un blog o un perfil en una red social, puedan publicar información que, en ocasiones, puede versar sobre la vida privada de otras personas. Por otro lado, los diarios han puesto a disposición de cualquier internauta sus hemerotecas digitalizadas con un doble objetivo: generar tráfico hacia sus sitios web y, en consecuencia, incrementar ingresos económicos a cambio de noticias, que pueden versar sobre la vida de personas, que ahora se ven expuestas a cualquiera que teclee su nombre en un buscador. El deseo de

A raíz del artículo de Warren y Brandeis, se obtuvieron diversas reacciones en los tribunales y legisladores, de forma que, en algunos Estados se admitió la posibilidad de entablar acciones en defensa de la protección de la privacidad, pero en otros no[23]. Setenta años después de la publicación del artículo, William L. Prosser publicó un estudio sobre unos trescientos casos judiciales relativos a la privacidad, que se habían planteado desde ese momento. Fruto de este análisis, Prosser concluyó que se podían dar cuatro tipos de acciones civiles (*torts*) contra la vulneración del derecho a la privacidad[24].

Asimismo, la formulación de la intimidad en clave de autodeterminación o *informational privacy* se atribuye al, también estadounidense, Alan F. Westin. Este autor la define como la capacidad que tienen los individuos de controlar cuándo, cómo y con qué alcance se comunica a otros la información sobre ellos mismos. Esta autodeterminación informativa encuentra límites en la propia voluntad del individuo que, por un lado, desea preservar su privacidad y, por otro lado, desea también mostrar esa información a otros, fruto de los usos sociales de la sociedad en la que vive[25]. Esta lucha

---

las personas afectadas de eliminar esta información, en lo que se conoce como el derecho al olvido, se enfrenta a derechos como el de la libertad de expresión y de información.

[23] Así, por ejemplo, el Estado de Nueva York estableció la acción (*tort*) de protección de la privacidad en una ley (la *New York Civil Rights Act, Section 51*), al haber denegado la Corte de Apelación el reconocimiento de la acción (*tort)* por invasión de la privacidad del *Common Law* (*Robertson v. Rochester Folding Box Co., 64 N.E. 442, New York 1902*). D.J. SOLOVE, P.M. SCHWARTZ, *Information Privacy Law, op.cit.*, págs. 25 a 27.

[24] Así estos cuatro *torts* o ilícitos civiles son, según W.L. PROSSER: "*1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs. 2. Public disclosure of embarrassing private facts about the plaintiff. 3. Publicity which places the plaintiff in a false light in the public eye. 4. Appropiation, for the defendant's advantage, of the plaintiff's name or likeness.*" Estos *torts* no han perdido su vigencia y se conocen como "*invasion of privacy*", denominándose respectivamente: *"(1) intrusion upon seclusion, (2) Public disclosure of private facts, (3) False light y (4) appropriation*". D.J. SOLOVE, P.M. SCHWARTZ, *Information Privacy Law, op.cit.*, págs. 27 a 28, que cita el artículo de W.L. PROSSER, "*Privacy*", *28 California Law Review, 383 (1960)*.

[25] Como señala R. MARTÍNEZ MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa, op. cit.*, pág. 80, nota al pie 55, que cita a A.F. WESTIN, *Privacy and freedom* (6ª ed.), Atheneum, New York, 1970, cuya primera edición se realizó en 1967, pág. 7: "*Privacy is the Claim of individuals, groups, or institutions to determine for themselves when, how, and to what extend information is communicated to others.""The individual's desire for privacy is never absolute, since participation in society is an equally powerful desire. Thus each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communications of himself to others, in light of the environmental conditions and social norms set by the society in which he lives. The individual does so in the face of pressures from the curiosity of others and from the processes of surveillance that every society sets in order to enforce its social norms*". Asimismo, cita también R. MARTÍNEZ MARTÍNEZ como exponente de esta construcción doctrinal de la *informational privacy* a los autores norteamericanos CH. FRIED y A.R. MILLER. Además, según indica PIÑAR MAÑAS la doctrina de WESTIN se recoge posteriormente en la importantísima sentencia sobre el censo, de 15 de diciembre de 1983, del Tribunal Constitucional Federal Alemán. De esta forma, el alto tribunal alemán elabora este derecho a la autodeterminación informativa que no se reconoce en la Ley Fundamental de Bonn de 1949 y

interna del individuo se halla presente en el actual contexto social, en una sociedad de la información donde la ciudadanía expone sus vidas en Internet, debido a la gran presión que origina el uso de plataformas de comunicación, como pueden ser las redes sociales[26]. Esto conlleva que el peso en la balanza actualmente se decante por el deseo de exponerse, antes que por el de preservar la privacidad[27].

---

encuentra su fundamento en el "derecho general de la personalidad" que sí se incluye en el artículo 2.1 de esta constitución. J. L. PIÑAR MAÑAS, "Protección de datos: origen, situación actual y retos de futuro", P. LUCAS MURILLO DE LA CUEVA, J.L. PIÑAR MAÑAS, *El derecho a la autodeterminación informativa*, *op. cit.*, págs. 88 a 90.

[26] Respecto a la preocupación sobre el uso de las redes sociales, especialmente por los menores, se puede citar el estudio que se llevó a cabo, durante dos años, por una Subcomisión creada a estos efectos por la Comisión de Interior del Congreso de los Diputados español y en la que participaron más de cien comparecientes. Entre las medidas propuestas, en el informe presentado en abril del 2015 como resultado del estudio, se pueden destacar las de naturaleza educativa que pretenden capacitar a los menores con las competencias digitales necesarias para ser ciudadanos digitales, así como para que utilicen de forma apropiada las redes sociales y sean conscientes de los peligros concretos que pueden encontrarse. Además de los menores también se propone educar a profesores, padres, así como a todos los que conforman la Administración de Justicia, las Fuerzas y Cuerpos de Seguridad y el personal socio-sanitario. Aprobación por la Comisión de Interior del Informe de la Subcomisión de estudio sobre las redes sociales, BOCG, Congreso de los Diputados, X Legislatura, serie D: general, número 643-1, de 9 de abril de 2015.

[27] Así P. SIBILIA se refiere a la obra autobiográfica de F. NIETZSCHE, *Ecce Homo ¿Cómo se llega a ser lo que se es?*, Buenos Aires, Elaleph.com, 2003, en la que el filósofo pretendía responder a esta pregunta y solicitaba a sus lectores que lo escucharan "pues yo soy tal y tal, ¡sobre todo, no me confundáis con otros!". En esa época se tachó a NIETZSCHE de megalómano y excéntrico y, sin embargo, la autora duda que hoy en día se consideraran estos adjetivos como algo negativo, como en aquella época. Considera SIBILIA que en esta época "se estimula la hipertrofia del yo hasta el paroxismo". Como ejemplos del concepto de extimidad que la autora toma prestado de Jacques Lacan pero al que brinda un nuevo significado (como opuesto a intimidad) alude SIBILIA a las redes sociales, los blogs, las webs como *Youtube*, donde se cuelgan vídeos. De esta forma, los diarios íntimos se han sustituido por los diarios éxtimos (los blogs), de forma que ahora se expone la intimidad en las vitrinas de la red. P. SIBILIA, *La intimidad como espectáculo,* Ed. electrónica, Fondo de Cultura Económica de Argentina, Buenos Aires, Argentina, 2012. SIBILIA además en una entrevista indica que las personas actualmente "cada vez nos definimos más a través de lo que podemos mostrar y que los otros ven. La intimidad es tan importante para mostrar lo que somos que hay que mostrarla. Eso confirma que existimos." C. PÉREZ-LANZAC, R. RINCÓN, "Tu extimidad contra mi intimidad", *El País Archivo*, 24.3.2009, http://elpais.com/diario/2009/03/24/sociedad/1237849201_850215.html (fecha consulta: 31.7.2013). De la misma forma, se puede citar la tendencia actual conocida como *quantified self*, originada en EEUU, consistente en la posibilidad de obtener información a través de objetos conectados a Internet (fenómeno que se conoce como *Internet of Things* o Internet de las cosas). De esta forma, una persona al pesarse en una balanza o al llevar un podómetro o unas zapatillas deportivas con sensores habilitados en las suelas, puede volcar esa información en Internet y gestionarla a través de programas informáticos, de forma que pueda controlar su estado físico. La evolución, actualmente incipiente, de esta tecnología preconiza nuevos modelos económicos y plantea la pregunta de que nuevos modelos de regulación exigirá, cuando además los datos que se tratan son datos sensibles, ya que la medicina es la primera que parece que está aprovechando estas posibilidades. S. VULLIET-TAVERNIER, "La quantified self: nouvelle forme de partage des données personnelles, nouveaux enjeux?", *IP Innovation & Prospective*, nº 5 juillet 2013, que además cita un informe del *Conseil général de l'économie, de l'industrie, de l'énergie et des technologies* (CGEIET), *Rapport "Bien vivre grâce au numérique" (2012) coordonné par* R. PICARD, disponible en www.cgeiet.economie.gouv.fr. La expresión *quantified self* o auto-medida es un movimiento que nace en 2007, en California, impulsado por Gary Wolf, uno de los editores de la revista *Wired*, y se caracteriza porque el propio usuario es el que genera los datos relativos a sus actividades para mejorar el conocimiento de si mismo. O. DESBIEY, "Le quantified self au coeur des nouvelles pratiques numériques de santé", *IP Innovation & Prospective*, nº 5 juillet 2013.

1.1.2. La legislación parcial y la autorregulación como mecanismos de protección del derecho a la privacidad en Estados Unidos

En el derecho positivo estadounidense y especialmente en su Constitución no se reconoce, en principio, expresamente el derecho a la intimidad[28]. Por eso, el Tribunal Supremo de este país lo construyó a partir de derechos reconocidos en el texto[29]. Hay que tener en cuenta que los derechos constitucionales, en el sistema estadounidense, se conciben como una limitación a la actuación de los poderes del Estado, no del sector privado[30].

Muestra de esta protección frente al Estado, es la primera norma que en EEUU regula la privacidad en el ámbito federal: la *Data Privacy Act* aprobada en 1974. Esta ley limita su ámbito de aplicación al tratamiento de información que realiza el gobierno federal. Hay que destacar el momento en el que el Congreso aprueba este texto, especialmente sensibilizado por el escándalo *Watergate* que precipitó la dimisión, por primera vez en la historia de EEUU, de su presidente, Richard Nixon[31]. Este escándalo demostró el alcance que podía llegar a tener el manejo por parte de los gobiernos de las

[28] Si bien algunas Constituciones estatales sí reconocen la protección de la privacidad, como la de Alaska (*Alaska Constitution, art. I, § 22*), la de California (*California Constitution art.1, § 1*) o la de Florida (*Florida Constitution art. I, § 23*). D.J. SOLOVE, P.M. SCHWARTZ, *Information Privacy Law*, *op.cit.*, págs. 35 a 36.

[29] Así explica MARTÍNEZ MARTÍNEZ que la Novena Enmienda de la Constitución de los EEUU opera como una cláusula de apertura a la incorporación de nuevos derechos. A su vez, la Decimocuarta Enmienda proporciona un argumento procesal para examinar los casos en que se planteen cuestiones relativas a la vida privada porque concede a los ciudadanos americanos el derecho a no ser privados de la vida, la libertad o la propiedad sin el debido proceso legal (*Due Process Clause*) que actúa como garantía de la libertad de los ciudadanos frente a los poderes del Estado. Estas dos cláusulas en relación con concretos derechos (libertad de expresión de la Primera Enmienda, límites al uso militar de las viviendas privadas en tiempos de paz en la Tercera Enmienda y protección del domicilio en la Cuarta Enmienda) han servido para inferir la presencia de la privacidad como derecho constitucional. R. MARTÍNEZ MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa*, *op. cit.*, págs. 103 a 133.

[30] En este sentido, MARTÍNEZ MARTÍNEZ menciona la crítica que realiza SCHWARTZ respecto a dejar en manos de la autorregulación de la industria la defensa de la privacidad de los ciudadanos, ya que considera que es necesario que sea el Estado el que mediante normativa proteja el acceso a la información personal de los usuarios de Internet, al estimar que en este entorno existen fuertes limitaciones a la autodeterminación informativa, como la existencia de contratos con la fórmula "lo tomas o lo dejas". R. MARTÍNEZ MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa*, *op. cit.*, pág.134 y págs. 84, 85. Como excepción a esta protección constitucional de la privacidad exclusiva frente a los Estados se menciona la de la Constitución de California (*California Constitution art.1, § 1*) que establece este protección expresamente frente al Estado pero también frente a actores del sector privado. D.J. SOLOVE, P.M. SCHWARTZ, *Information Privacy Law*, *op.cit.*, págs. 35 a 36.

[31] *Overview of the Privacy Act of 1974*, *Department of Justice's Office of Privacy and Civil Liberties*, en http://www.justice.gov/opcl/1974privacyact-overview.htmp (fecha de consulta: 20.1.2013), pág. 7; A. TÉLLEZ AGUILERA, *La Protección de datos en la Unión Europea: divergencias normativas y anhelos unificadores*, Edisofer, Madrid, 2002, pág. 22 y M. ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, Tirant lo blanch, Valencia, 2006, pág. 275.

tecnologías y la necesaria protección de los ciudadanos frente a estas agresiones. Posteriormente, se aprobaron a escala federal otras leyes que también protegen la privacidad frente al uso de la información que pueda realizar el gobierno[32].

Fruto de los trabajos preparatorios de la *Data Privacy Act* se elaboró un informe para evaluar las consecuencias de la utilización de sistemas informáticos para el tratamiento de datos personales y para sugerir recomendaciones respecto a mecanismos de tutela frente a las posibles consecuencias negativas[33]. Como resultado del estudio realizado, se concluyó que la privacidad no estaba suficientemente protegida frente al mal uso de los sistemas automatizados y se recomendó la adopción de un código de buenas prácticas (*Code of Fair Information Practice*).

El código descansaría sobre unos principios básicos, conocidos como los *Fair Information Practice Principles* (FIPPs)[34]. Estas principios se utilizaron, según múltiples informes, como inspiración para otras normas o instrumentos jurídicos, como la Guía de la Organización de Cooperación y Desarrollo Económico relativa a la protección de la privacidad y de las transferencias de datos personales (Guía OCDE 1980), el Convenio 108, el *Asia-Pacific Economic Cooperation Privacy Framework (*APEC Privacy

[32] Así en 1978 se aprobó la *Right to financial privacy Act* que limita las comunicaciones de datos de las entidades financieras al gobierno, en 1980 se aprobó la *Privacy Protection Act* que protege la información que obra en poder de los periodistas también frente a posibles interferencias por parte del gobierno, en 1986 la *Electronic Communications Privacy Act* que regula la interceptación de comunicaciones por el gobierno, en 1994 la *Drivers Privacy Protection Act* que protege los datos del registro de tráfico. También hay una batería de normas que persiguen asegurar la seguridad de la información que trata el gobierno federal: la *Computer Fraud and Abuse Act* de 1986 y la *Federal Information Security Management Act*.

[33]*Records computers and the rights of citizens, report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education & Welfare, July 1973.* http://www.justice.gov/sites/default/files/opcl/docs/rec-com-rights.pdf (fecha consulta: 30.7.2014).

[34] *The fair information practice principles: framework for privacy policy at the Department of Homeland Security, Privacy policy guidance memorandum 2008-01, The Privacy Office, U.S. Department of Homeland Security,* 29.12.2008, http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (fecha consulta: 4.1.2015); *Consumer data privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy,* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf, (fecha consulta: 2.8.2014), pág. 9*; Big Data: seizing opportunities, preserving values, Executive Office of the President, The White House, 1.5.2014,* pág.17, http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf. (fecha consulta: 4.1.2015). No obstante, es difícil determinar la fuente de inspiración de los diferentes instrumentos jurídicos que han regulado la protección de datos, ya que la preparación de los mismos se ha realizado, en muchas ocasiones, en paralelo. Así, por ejemplo, en el mismo informe que se cita como el origen de estos FIIPs se estudiaron los trabajos que otros comités habían efectuado para otros procesos. Así se citan informes del gobierno de Canadá o el de un comité sueco para la elaboración de la primera ley sueca de protección de datos que se aprobó al mismo tiempo que se presentó el informe estadounidense. *Records computers and the rights of citizens, op. cit.*, pág. x.

Framework*)*, la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE de Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (Decisión *Safe Harbour*) e incluso se menciona la Directiva 95/46/CE[35].

Aunque en la regulación estadounidense prime la protección frente al gobierno, también se ha legislado para proteger a los individuos de las agresiones propiciadas por las empresas[36]. No obstante, estas leyes se refieren a sectores muy concretos[37] y no tienen un alcance general[38]. De hecho, una de estas normas también se ha considerado un

[35] Estos cinco principios básicos eran: "*There must be no personal data record-keeping systems whose very existence is secret. There must be a way for an individual to find out what information about him is in a record and how it is used. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent. There must be a way for an individual to correct or amend a record of identifiable information about him. Any organization creating, maintaining, using, or diseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data*". Estos principios, a su vez, se desarrollarían mediante unas medidas que serían los estándares mínimos que deberían adoptarse en la gestión de los sistemas informáticos y que configurarían las buenas prácticas (las *fair information practices*). Las medidas que se desglosaban en el informe incluían requisitos generales, requisitos de información que debía hacerse pública sobre el sistema informático y derechos que se brindaban a los sujetos cuyos datos se trataban. *Records computers and the rights of citizens, op. cit.*, págs. xx a xxxii.

[36] Se puede hallar un listado de las leyes federales más relevantes para la protección de la privacidad en A. QUESADA RODRÍGUEZ, *Protección de datos y telecomunicaciones convergentes, Premio protección de datos personales de investigación 2014*, Agencia Española de Protección de Datos, Agencia Estatal BOE, Madrid, 2015, págs. 278 a 304.

[37] Ejemplos de estas normas sectoriales son: *Cable Communications Policy Act* de 1984, que regula el tratamiento de datos que pueden realizar los servicios por cable, la *Telephone Consumer Protection Act* de 1991, que protege a los consumidores de llamadas no solicitadas y la *Telecommunications Act* de 1996, que incluye previsiones para asegurar que los proveedores de servicios de telecomunicaciones protejan la privacidad de los datos de los clientes; *Family Educational Rights and Privacy Act* de 1974, que protege los datos de los expedientes académicos de los alumnos de estos centros; *Children's Online Privacy Act* de 1998; *Video Privacy Protection Act* de 1988, que se aprobó a raíz de la publicación en un periódico de la información de los vídeos alquilados por un candidato al Tribunal Supremo, Robert Bork, por lo que también se conoce como "*Bork Bill*", D.J. SOLOVE, P.M. SCHWARTZ, *Information Privacy Law, op.cit.*, pág. 840; *Employee Polygraph protection Act* de 1988, que limita el uso de polígrafos como requisito de contratación y *Gramm-Leach-Bliley Financial Services Modernization Act* de 1999.

[38] SCHWARTZ plantea si es conveniente que en EEUU se apruebe una ley ómnibus en materia de privacidad a nivel federal que primara sobre las legislaciones aprobadas por los Estados. El autor compara las diferentes aproximaciones que a nivel normativo han adoptado los EEUU y la UE. En los EEUU han optado por establecer respecto al sector privado leyes sectoriales de protección de la privacidad y únicamente una ley federal en el ámbito público pero de alcance limitado a determinadas agencias. Esta vía da mayor libertad a los Estados para legislar sobre la materia. En cambio en la UE se ha optado por adoptar una ley generalista, la Directiva 95/46/CE que deben transponer los Estados miembros. El autor analiza las razones que han llevado a esta aproximación diversa. En EEUU podríamos tener ahora un panorama legislativo diferente si se hubiera aprobado un proyecto de ley ómnibus para los dos sectores público y privado que se presentó el 1 de mayo de 1974 por el Senador Samuel Ervin (*Senate Bill 3418*). Este proyecto establecía que su ámbito de aplicación subjetivo era: "*any Federal agency, State or local*

antecedente de las posteriores regulaciones sobre tratamiento de datos mediante sistemas informáticos[39]. Se trata de la *Fair Credit Reporting Act*, de 26 de octubre de 1970 (previa, por tanto, a la *Data Privacy Act*) que regulaba la gestión de informes sobre la solvencia de las personas[40]. Esta ley establece un sistema que implica, por un lado, establecer las obligaciones de las empresas que se dedican a esta actividad y, por otro lado, establecer los derechos que tienen los afectados, como el de acceso a la información que estas empresas mantienen. Obligaciones y derechos, por tanto, que serían después trasladados a las normas sobre tratamiento de datos.

Ni la *Data Privacy Act* ni estas normas sectoriales recogen una noción general de responsable, tal como se configura en la normativa europea. La razón cabe encontrarla en que no se pretende un régimen generalizado que abarque todos los sectores y operadores que puedan tratar datos. El hecho de instaurar una figura, como la del responsable, obedecería a la necesidad de tipificar una categoría de sujetos, con el fin de facilitar su determinación en múltiples contextos. Sin embargo, como todas las leyes, estas normas sectoriales deben delimitar su ámbito de aplicación y los sujetos obligados a cumplirlas y a responder de los incumplimientos[41].

---

government, or any other organization maintaining an information system that includes personal information". Por tanto, este proyecto, al establecer este ámbito subjetivo delimitaba los sujetos obligados, de forma que hallaríamos un desglose de los posibles sujetos bastante generalista, el hecho caracterizador de que estos sujetos debían mantener un sistema de información y el elemento objetivo que sería la información personal. Sin embargo, esta ley no se llegó a aprobar y se optó por legislar de forma sectorial. Las razones de que no se optara por esta ley ómnibus en los años setenta, considera el autor que podrían ser las dudas sobre si el sector privado ponía en peligro la privacidad o lo que denomina "parsimonia reguladora" ("*regulatory parsimony*") ante el temor de que se pudiera restringir la actividad de las organizaciones. De otro lado, para el autor la UE requería de una solución uniforme que facilitara la integración de los diferentes Estados miembros que se unían a la organización. El autor considera que no sería positiva la aprobación de una ley ómnibus federal ya que no permitiría la flexibilidad y la adaptación a la evolución tecnológica que sí permiten modelos más ágiles de normas sectoriales y estatales. Sin embargo, el autor considera que una ventaja de la ley ómnibus federal y prevalente sería la de establecer definiciones que determinarían su alcance y que evitarían que los Estados modificaran el mismo. SCHWARTZ, P.M., "Preemption and privacy*"*, *The Yale Law Journal*, 118:902, 2009, págs. 902 a 947.

[39] Así lo estima P. LUCAS MURILLO DE LA CUEVA, *El derecho a la autodeterminación informativa (La protección de los datos personales frente al uso de la informática), op. cit.*, pág.126, donde en nota al pie 35 cita a R. R. STAUFFER, "*Tenant Blacklisting: Tenant screening services and the right to privacy*", *Harvard Journal on Legislation*, vol. 24, nº 1, 1987, pág. 251.

[40] Esta norma pionera se aprobó con el fin de limitar una industria, la de servicios de información sobre solvencia, muy importante y que originó una gran polémica en los años sesenta debido a graves abusos cometidos por algunas de estas empresas que incluían informaciones negativas o incompletas en sus fichas, así como datos sensibles acerca de la orientación sexual o del estilo de vida, fichas que se vendían a compañías de seguros y empleadores que las utilizaban para denegar sus servicios o puestos de trabajo a los ciudadanos, sin que estos pudieran siquiera tener acceso a estas informaciones, http://epic.org/privacy/fcra/ (fecha de consulta 20.1.2013).

[41] Hay que mencionar el concepto de "operador" que se incluye en una ley federal de 1998 que persigue la protección de los menores en el entorno de Internet. Si bien no incluye exactamente los elementos que

¿El hecho de que el sistema estadounidense haya optado por leyes sectoriales facilita la delimitación de este sujeto obligado? Pues parece que no se puede dar una respuesta afirmativa. Como ejemplo de esta dificultad se puede citar la *Data Privacy Act*, que establece como principal sujeto obligado a las agencias gubernamentales federales. Para ello se incluye en la ley una definición de lo que se considera agencia y que ha tenido que ser interpretada por los tribunales para determinar qué sujetos deben entenderse incluidos en la misma[42].

---

luego se verá que integran el concepto de responsable incluido en la normativa europea, se aproxima al mismo. El operador sería el sujeto obligado que trata datos de los menores y se define como cualquier persona que gestione un sitio web o un servicio *online* y que recoga o mantenga datos personales sobre los usuarios de este sitio web o servicio, o en nombre de quien se recojan o mantengan datos. Se puede ver que esta norma incluye una definición de sujeto obligado amplia y que se refiere a la posibilidad de encomendar la gestión de la información a otros, rasgo que, como se verá, caracteriza al responsable. Es decir que contempla la opción de que sea otro el tratador efectivo de la información. A continuación se reproduce esta definición: *"2) Operator. The term "operator" (A) means any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce (i) among the several States or with 1 or more foreign nations; (ii) in any territory of the United States or in the District of Columbia, or between any such territory and (I) another such territory; or (II) any State or foreign nation; or (iii) between the District of Columbia and any State, territory, or foreign nation; but (B)does not include any nonprofit entity that would otherwise be exempt from coverage under section 45 of this title", Section 1302(2) Children's Online Privacy Protection Act of 1998 (COPPA).*

[42] Así, por ejemplo se pueden ver casos planteados en los que se determina cuándo los trabajadores de las agencias pueden ser considerados responsables. *Overview of the Privacy Act of 1974, op. cit.*, págs. 4 a 14. También se puede mencionar la *Video Privacy Protection Act* (VPPA) que define lo que considera *Video Tape Service Provider* (proveedor de servicios de cintas de vídeo), como el sujeto obligado. En el asunto *Dirkes v. Borough of Runnemede, 936 F. Supp. 235 (D.N.J. 1996)* se planteó si la VPPA se podía aplicar a sujetos que no se podían considerar dentro de esta categoría. En concreto, se cuestionaba si se podía aplicar la norma a un policía que había obtenido de uno de estos proveedores el listado de las cintas de vídeo alquiladas por el afectado sin ninguna orden y que se presentó en un juicio. El tribunal, en este caso, entendió que la ley debía interpretarse de forma amplia para incluir a este policía. En cambio, en otro asunto, *Daniel v. Cantell 375 F.3d 377 (6th Cir. 2004),* ante un supuesto similar, el tribunal refutó esta interpretación y entendió que no podía ampliarse la aplicación de la ley a sujetos que no fueran los incluidos en la definición de *Video Tape Service Provider.* Como indica el tribunal, si cualquier persona pudiera ser considerada responsable bajo esta ley, no habría necesidad de incluir una definición que limitara a los sujetos obligados a cumplirla. En referencia a la *Electronic Communications Privacy Act*, se puede citar el asunto *Dyer v. Northwest Airlines Corp. 334 F. Supp. 2d 11 96 (D.N. 2004),* en el que se demandó a la compañía aérea *Northwest Airlines Corp*. por entregar los datos de pasajeros a la *National Aeronautical and Space Administration* (NASA) tras los atentados del 11S. El tribunal entendió que no se podía aplicar esta norma a la compañía aérea, ya que su ámbito de aplicación se dirigía a los proveedores de servicios de acceso a Internet y de telecomunicaciones y no a negocios que tradicionalmente se dedicaban a vender servicios o productos a través de Internet. D.J. SOLOVE, P.M. SCHWARTZ, *Information Privacy Law*, *op.cit.*, págs. 840 a 846, 857 a 858.

1.1.3. La libertad de expresión, la seguridad y el mercado, aspectos que modulan la protección de la privacidad en Estados Unidos

La comprensión del contexto en el que se desarrolla la protección de la privacidad exige añadir otros elementos clave en la cultura americana: la libertad de expresión, la seguridad y el capitalismo.

La libertad de expresión, incluida en la Primera Enmienda de la Constitución americana, se erige en este país, como derecho preferente en su ordenamiento y, por lo tanto, se primará normalmente por encima de otros derechos como el de privacidad[43].

Así, cuando en 1995 se inició la utilización por el público de Internet, hasta ese entonces una red creada en un entorno militar y utilizada en el ámbito científico, se produjo un primer intento de regulación de este nuevo espacio de comunicación. En 1996 se aprobó la *Communications Decency Act* que restringía la transmisión de material obsceno, indecente u ofensivo, especialmente a menores, por medios de telecomunicación[44]. El objetivo de esta ley era el de proteger a los niños de los problemas de pederastia y pornografía infantil que se conocieron y se contemplaban incluso penas privativas de libertad.

Empezó un debate nacional en el que, de un lado, los partidarios de la libertad en Internet, los defensores de la libertad de expresión, tacharon la norma de inconstitucional, la veían como un modo de censura y, del otro lado, se hallaban los defensores de los menores[45].

[43] Ejemplo de la relevancia que este país otorga a esta libertad, en contraposición con la postura de Europa, es el diferente tratamiento de la incitación al odio. La Corte Suprema norteamericana ha estimado que una expresión odiosamente racista no debe castigarse sólo porque una comunidad se vea ofendida por el mensaje, salvo si existe un peligro claro e inmediato de causar daños concretos. Contrariamente, en el ámbito del Consejo de Europa se ha entendido que las manifestaciones racistas no están amparadas por la libertad expresión. En esta misma línea, nuestro Tribunal Constitucional ha declarado que en una actitud racista no hay valor informativo ni cultural y, por tanto, no cabe dentro de la libertad expresión (STC 176/1995, de 11 de diciembre, caso Hitler=SS, FJ 5). M.J. GARCÍA MORALES, "Libertad de expresión y control de contenidos en Internet", P. CASANOVAS ROMEU (Ed.), *Internet y pluralismo jurídico: Formas emergentes de regulación*, Comares, Granada, 2003, págs. 33 a 39.

[44] *Ibídem*, págs. 37 a 39.

[45] En este contexto J. PERRY BARLOW, co-fundador de la *Electronic Frontier Foundation*, proclamó en Davos, el ocho de febrero de 1996 la Declaración de Independencia del Ciberespacio, dirigida a los Estados, en la que se ilustraba el ideario libertario que aún hoy permanece vigente: "Gobiernos del Mundo Industrial, vosotros, cansados gigantes de carne y acero, vengo del Ciberespacio, el nuevo hogar de la Mente. En nombre del futuro, os pido en el pasado que nos dejéis en paz. No sois bienvenidos entre

El resultado de esta oposición fue la interposición de recursos ante los tribunales y finalmente, en sentencia del Tribunal Federal de Pensilvania, se declaró el 12 de junio de 1996 la inconstitucionalidad de la ley. Se recurrió ante el Tribunal Supremo que confirmó la sentencia el 27 de junio 1997. En esta sentencia el Alto Tribunal entendió que Internet era un nuevo medio que democratizaba la información en el que cualquier usuario podía emitir información y este aspecto debía ser protegido[46]. Por tanto, se puede decir que ganó la libertad de expresión.

Respecto a la seguridad, cuando Internet se empezó a implantar en el resto del mundo los gobiernos empezaron a ser conscientes de las amenazas que podía implicar este nuevo entorno, como el cibercrimen. La diversidad de jurisdicciones implicadas y leyes aplicables hacían muy difícil luchar contra este fenómeno. La armonización a nivel internacional de las normativas se convirtió en una de las opciones que barajaban los gobiernos para aunar esfuerzos en esa lucha y en el año 2001 se aprobó el Convenio de

---

nosotros. No ejercéis ninguna soberanía sobre el lugar donde nos reunimos. No hemos elegido ningún gobierno, ni pretendemos tenerlo, así que me dirijo a vosotros sin más autoridad que aquella con la que la libertad siempre habla. Declaro el espacio social global que estamos construyendo independiente por naturaleza de las tiranías que estáis buscando imponernos. No tenéis ningún derecho moral a gobernarnos ni poseéis métodos para hacernos cumplir vuestra ley que debamos temer verdaderamente. Los gobiernos derivan sus justos poderes del consentimiento de los que son gobernados. No habéis pedido ni recibido el nuestro. No os hemos invitado. No nos conocéis, ni conocéis nuestro mundo. El Ciberespacio no se halla dentro de vuestras fronteras. No penséis que podéis construirlo, como si fuera un proyecto público de construcción. No podéis. Es un acto natural que crece de nuestras acciones colectivas. No os habéis unido a nuestra gran conversación colectiva, ni creasteis la riqueza de nuestros mercados. No conocéis nuestra cultura, nuestra ética, o los códigos no escritos que ya proporcionan a nuestra sociedad más orden que el que podría obtenerse por cualquiera de vuestras imposiciones. Proclamáis que hay problemas entre nosotros que necesitáis resolver. Usáis esto como una excusa para invadir nuestros límites. Muchos de estos problemas no existen. Donde haya verdaderos conflictos, donde haya errores, los identificaremos y resolveremos por nuestros propios medios. Estamos creando nuestro propio Contrato Social. Esta autoridad se creará según las condiciones de nuestro mundo, no del vuestro. Nuestro mundo es diferente. El Ciberespacio está formado por transacciones, relaciones, y pensamiento en sí mismo, que se extiende como una quieta ola en la telaraña de nuestras comunicaciones. Nuestro mundo está a la vez en todas partes y en ninguna parte, pero no está donde viven los cuerpos. Estamos creando un mundo en el que todos pueden entrar, sin privilegios o prejuicios debidos a la raza, el poder económico, la fuerza militar, o el lugar de nacimiento. Estamos creando un mundo donde cualquiera, en cualquier sitio, puede expresar sus creencias, sin importar lo singulares que sean, sin miedo a ser coaccionado al silencio o al conformismo. Vuestros conceptos legales sobre propiedad, expresión, identidad, movimiento y contexto no se aplican a nosotros. Se basan en la materia. Aquí no hay materia. (…). Crearemos una civilización de la Mente en el Ciberespacio. Que sea más humana y hermosa que el mundo que vuestros gobiernos han creado antes." http://es.wikisource.org/wiki/Declaraci%C3%B3n_de_independencia_del_ciberespacio, (fecha consulta: 28.11.2014).

[46] Dicha norma se declaró inconstitucional en esta sentencia por entender el tribunal que las medidas previstas eran desproporcionadas, ya que la protección de los menores podía conseguirse con medios menos restrictivos de la libertad de expresión. M.J. GARCÍA MORALES, "Libertad de expresión y control de contenidos en Internet", P. CASANOVAS ROMEU (Ed.), *Internet y pluralismo jurídico: Formas emergentes de regulación*, *op. cit.*, págs. 37 a 39.

cibercriminalidad, en el seno del Consejo de Europa, cuya firma se abrió a países no miembros, como EEUU[47].

Tras los atentados terroristas de 2001, EEUU aprobó la polémica *USA Patriot Act* que reformó las normas procesales para facilitar la lucha del Estado contra el terrorismo y que afectó a algunas de las normas que protegían la privacidad referenciadas anteriormente[48]. Se ampliaron las posibilidades de espionaje para las fuerzas de seguridad, se establecieron hasta veinte años de cárcel y cadena perpetua en caso de muertes o atentados contra infraestructura.

El continente europeo fue sacudido también por los atentados terroristas de Madrid y Londres, en los años 2004 y 2005, respectivamente. Por ello, la UE, entre otras medidas, aceptó la suscripción de un acuerdo para que las compañías aéreas proporcionaran datos de los pasajeros que viajaban a EEUU[49].

---

[47] Anteriormente se habían aprobado varias recomendaciones en el seno del Consejo de Europa, con el fin de promover la lucha contra los delitos que se habían propiciado en el entorno digital: Recomendación nº R(89) 9 sobre delitos informáticos y Recomendación nº R(95) 13 concerniente a los problemas procesales penales conectados con la tecnología de la información, adoptadas en 1989 y 1995 respectivamente. También en el marco de la Organización de Naciones Unidas se habían aprobado las resoluciones 55/63 de 4 de diciembre de 2000 y 56/121 de 19 de diciembre de 2001 sobre la lucha contra el uso de la tecnología para cometer delitos.

[48] Como ejemplo y respecto a la *Electronic Communications Privacy Act* de 1986 además de que esta norma no prohíbe a los operadores la comunicación de datos de sus abonados a terceros, expresamente establece que si el operador razonablemente estima que existe una situación de emergencia que implica peligro de muerte o de daños graves para alguna persona podrá realizar esa comunicación de datos, autorización que se establece en el apartado 2702 introducida por la *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (conocida como *USA PATRIOT ACT*). http://epic.org/privacy/ecpa/ (fecha consulta: 21.1.2013).

[49] Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, DO L 215/5 de 11.8.2012. Este acuerdo sustituyó al acuerdo previo de 23 y 26 de julio de 2007 que era de aplicación provisional, como resultado de la anulación por parte del TJUE de la Decisión 2004/496/CE del Consejo, de 17 de mayo de 2004, relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos, y la Decisión 2004/535/CE de la Comisión, de 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos. El TJUE entendió que la Decisión 2004/535/CE de la Comisión se refería a un tratamiento de datos personales que estaba fuera del ámbito de aplicación de la Directiva 95/46/CE, de acuerdo con la exclusión de su artículo 3.2, ya que su finalidad era la prevención y lucha contra el terrorismo y delitos graves. Respecto a la Decisión 2004/496/CE del Consejo, el TJUE consideró que no se había elegido correctamente la base jurídica (el artículo 95 CE) que se refería al establecimiento del mercado interior, ya que, de nuevo, la finalidad de la decisión era la ya apuntada. Sentencia del TJUE de 30 de mayo de 2006, *Parlamento Europeo/Consejo de la Unión* Europea y Comisión C-317/04 y C-318/04, EU:C:2006:346. Respecto a estos acuerdos el GA29 ha sido muy crítico, lo que puede verse en los numerosos documentos emitidos por este grupo con números WP 53, 66, 78, 87, 95, 97, 122, 124, 132, 138, 145, 151, 178, 181.

Desde el punto de vista económico, la aparición de la informática y de Internet originó nuevos modelos de negocio, que supusieron para EEUU el liderazgo de la industria en el contexto digital. La fragmentada legislación que protegía la privacidad se complementó con el impulso de la autorregulación en el sector empresarial. Esta opción permitía flexibilidad a las empresas que eran las que decidían someterse a las buenas práctica y que también podían decidir sobre los concretos mecanismos de cumplimiento. No obstante, con el fin de asegurar el cumplimiento de este compromiso, asumido por estas empresas, la *Federal Trade Commission* tenía la capacidad de perseguir los incumplimientos de estas buenas prácticas[50].

De esta forma, este sistema autorregulatorio también fue el instaurado para posibilitar que las empresas europeas pudieran transferir datos personales a las empresas estadounidenses. Pese a que existía normativa estadounidense que protegía el derecho a la privacidad, no era un cuerpo legislativo uniforme en todo el país y que protegiera frente a todos los operadores privados. Por lo tanto, no era posible que la UE considerara, en virtud de esta normativa a EEUU un país que cumpliera el nivel adecuado de protección de los datos personales, de acuerdo con lo establecido en su Directiva 95/46/CE[51]. Por eso, la Comisión Europea aprobó la Decisión *Safe Harbour*, en el 2000, donde se establecían unos principios a los que se podían acoger voluntariamente las empresas estadounidenses, que entonces se consideraba que contaban con el nivel adecuado de protección de datos[52]. Las empresas europeas podían transferir datos personales a estas

[50] La FTC actúa en defensa de la privacidad a través de la prohibición de "*unfair or deceptive acts or practices*" establecida en la *FTC Act Section 5*. Así puede interponer acciones civiles contra empresas que no cumplen por ejemplo con los principios de la Decisión *Safe Harbour* o que no cumplen con los compromisos que publicitan como compañías que otorgan sellos, como *True Ultimate Standards Everywhere Inc*, de nombre comercial TRUSTe. Esta empresa otorga sellos a sitios web que muestran que sus políticas de privacidad cumplen con una serie de requisitos que son evaluados por esta empresa. La FTC inició acciones contra la misma a finales de 2014, al denunciarse que TRUSTe no cumplía con su compromiso de revisar anualmente que los sitios web cumplían con los requisitos para mantener la certificación. http://business.ftc.gov/blog/2014/11/ftcs-truste-case-when-seals-help-seal-deal (fecha consulta: 2.1.2015).

[51] Como indica SCHWARTZ, en marzo de 2007, Bill Gates, presidente de *Microsoft* reclamó que se promulgara una ley federal que protegiera la privacidad de forma general. A esta iniciativa se sumaron las principales empresas tecnológicas estadounidenses. Entre los argumentos que esgrimían estas compañías estaba la armonización de las aproximaciones normativas de EEUU y la UE, de forma que se minimizaran los conflictos en este ámbito respecto a las transferencias internacionales de datos. P.M. SCHWARTZ, "Preemption and privacy*", The Yale Law Journal, op. cit.*, pág. 904.

[52] Así se especifica en la decisión que considera que aunque los EEUU y la UE compartan el objetivo de mejorar la protección de la vida privada de sus ciudadanos, los EEUU siguen un enfoque diferente al europeo, de forma que su planteamiento es sectorial y se fundamenta en una mezcla de legislación,

empresas sin tener que solicitar autorización para ello a las autoridades de control de protección de datos.

En febrero de 2012 el presidente de EEUU, Barack Obama, presentó el documento *Consumer data privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy*[53], que pretendía suplir las carencias señaladas de la protección de la privacidad en EEUU. De esta forma, el documento contenía el plan de actuación de la Casa Blanca a escala federal para proteger la privacidad de los estadounidenses frente al sector privado que utilizaba sus datos para fines comerciales. En ese momento se acababa de iniciar el proceso de reforma de la Directiva 95/46/CE en Europa y estaba en marcha la reforma de la Guía de la OCDE y el Convenio 108.

El objetivo del plan era preservar la confianza de los consumidores mediante la protección de su privacidad en una sociedad interconectada. Esta confianza se vislumbraba como factor esencial para que las empresas estadounidenses continuaran siendo líderes en innovación de servicios tecnológicos.

La estrategia plasmada en el documento constaba de cuatro elementos: una declaración de derechos sobre la privacidad de los consumidores (*Consumer Privacy Bill of Rights* o CPBR) cuya intención era que se transformara en una ley federal, el desarrollo de códigos de conducta que tomara como base la CPBR[54], reforzar la protección mediante la acción de la *Federal Trade Commission* y la mejora de la interoperabilidad con otras instancias internacionales. La CPBR incluye los FIPPs pero adaptados al actual contexto.

Y es que cuando parecía que la tendencia era a que en la balanza pesara más la seguridad ante los atentados terroristas y menos la protección de la privacidad, se había iniciado una vuelta de tuerca. La balanza empezó a oscilar a favor de la protección del derecho, con el proceso para adaptar los instrumentos jurídicos que lo regulaban a los

---

reglamentación y autorregulación. Por ello, se optó por establecer unos principios a los que las empresas estadounidenses podían acogerse voluntariamente y obtener la presunción de adecuación, con el fin de facilitar que empresas europeas les transfiriesen datos personales. Decisión *Safe Harbour*, Anexo I.

[53] http://www.whitehouse.gov/sites/default/files/privacy-final.pdf, (fecha consulta: 2.8.2014)

[54] De esta forma, se afirmaba que, incluso si el Congreso no aprobaba la ley proyectada, se podía utilizar la CPBR como un modelo para incrementar la protección de la privacidad en Internet. Se reflejaba, por tanto, que iba a ser difícil aprobar una ley.

cambios tecnológicos. Además, desde la UE, se puso en duda la validez de los mecanismos regulatorios de las transferencias de datos con destino a EEUU[55].

Esta vuelta de tuerca llegó a su punto álgido con las filtraciones que se produjeron a mediados de 2013 acerca de los programas de espionaje que llevaba a cabo EEUU[56]. Las consecuencias de estas filtraciones han originado aún más tensión entre Europa y EEUU con respecto a la protección de datos. Al mismo tiempo, estas filtraciones han introducido otro elemento en el debate: la transparencia. Esta necesidad de transparencia se ha visto acrecentada por el crecimiento de los datos volcados, por la generación de un saber social que las personas consideran como un bien común que debe ser accesible a todos[57].

---

[55] Ver Capítulo VIII.

[56] Después de las filtraciones conocidas a través del portal *Wikileaks* que desvelaron informaciones secretas relativas al gobierno de los EEUU, de las que el responsable fue el joven soldado Bradley Manning, el 9 de junio de 2013, Edward Snowden, un consultor, ex agente de la CIA, que trabajaba para *Booz Allen Hamilton*, empresa subcontratada por el Estado de EEUU, en una entrevista del periódico *The Guardian* afirmó ser la fuente de las informaciones que en esos días se habían publicado en los periódicos *The Guardian* y *Washington Post* sobre los programas de espionaje masivo que llevó a cabo la Agencia de Seguridad Nacional de los Estados Unidos (la NSA). Según la información que publica theguardian.com (*Essential guide*) lo que movió a Snowden a filtrar información fue la necesidad de que se generara un debate sobre los límites de esta vigilancia. Además de la NSA, también estaba implicada la GCHQ (*Government Communications Headquarters*), la agencia equivalente a la NSA en el Reino Unido. Snowden informó sobre los diferentes programas de espionaje utilizados por estas agencias. El más conocido es PRISM, un programa de vigilancia de la NSA (pero al que también se da acceso a la GCHQ) que consiste en el acceso a los datos contenidos en los servidores de las principales empresas tecnológicas estadounidenses como *Google*, *Apple*, *Microsoft*, o *Facebook*. Ambas agencias también tienen programas de interceptación masiva de los cables de fibra óptica en el interior del Reino Unido y de EEUU, de forma que se capta toda la información que entra y sale de estos países. De igual forma, se interceptan los cables submarinos que conectan con el resto del mundo. De esta forma se accede a ingentes volúmenes de información telefónica y de Internet. También se conoció el programa de captación de datos de tráfico por la NSA de las llamadas telefónicas de millones de norteamericanos y los programas de ambas agencias para socavar los sistemas de cifrado que protegen las comunicaciones en Internet. La NSA cuenta con un presupuesto anual de 250 millones de dólares para invertir en analizar y poder contrarrestar los sistemas de seguridad tecnológicos. También se informaba del programa *Xkeyscore*, mediante el que se podían lanzar búsquedas con el único dato de un e-mail o p.ej. con el nombre de usuario de una red social y obtener acceso a todos los e-mails (incluyendo el contenido de los mismos) de esa dirección o a toda la información de los chats o mensajes privados del usuario de *Facebook*, respectivamente. También permitía esta herramienta acceder a toda la información de la navegación de un usuario por Internet. Según esta noticia se exige orden judicial para poder interceptar las comunicaciones de ciudadanos estadounidenses pero se permite esta interceptación si estos ciudadanos se comunican con extranjeros y, evidentemente, se permite la misma respecto a todo el que no sea ciudadano estadounidense. G. GREENWALD, "*XKeyscore: NSA tool collects' nearly everything a user does on the Internet*", 31.7.2013, http://theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data/print y *Essential guide*, theguardian.com (fecha consultas: 31.7.2013).

[57] Así lo indica RODOTÁ que resalta que estas filtraciones se han legitimado con la mediación de los periódicos que han servido de cauce para proporcionar la información facilitada. Han sido, por tanto, estas empresas las que han tenido que ponderar los derechos fundamentales afectados, entre los que figuraba el de protección de datos. En respuesta a esta demanda de transparencia los Estados ofrecen a sus ciudadanos legislaciones que permiten el acceso a la información de las administraciones públicas. Sin embargo, como reclama este autor hubiera sido preciso un proceso de reflexión en el que se hubiera tenido que valorar la

Los atentados de Francia, a principios del año 2015, parecía que, de nuevo, iban a acercar más a los legisladores hacia la seguridad. En este contexto, tres años después de publicar su estrategia sobre privacidad, el Presidente de EEUU presentó el borrador de la ley federal sobre el derecho a la privacidad de los consumidores[58]. En este borrador aparece un listado de definiciones, entre las que figura la de las "entidades incluidas" (*covered entity*). Esta definición se puede asimilar a la de responsable de nuestra regulación pero cuenta con importantes diferencias[59].

Como se verá a continuación, la sistemática que actualmente está vigente en EEUU se contrapone con la opción seguida en Europa y algunos instrumentos internacionales que han preferido una concepción generalista de la normativa y, como consecuencia de esta perspectiva han erigido a la figura del responsable como eje de la misma. La cultura jurídica europea refleja además la consecución del reconocimiento de unos derechos que se colocan en los cimientos de los ordenamientos y que, si bien, hayan sus límites en otros derechos de momento, resisten mejor la tensión frente a la libertad de expresión o las necesidades surgidas de la falta de seguridad. No obstante, dichos derechos también se ven a veces víctimas de la globalización debido a la presión de EEUU por extender sus valores e intereses.

1.2. El Convenio Europeo de Derechos Humanos: Los cimientos de la protección de datos personales en Europa

Antes de entrar en el análisis de las primeras definiciones del responsable, hay que mencionar las primeras bases jurídicas utilizadas para desarrollar posteriormente la regulación del derecho a la protección de datos. La primera de estas bases de la regulación europea se halla en el artículo 8.1 CEDH[60] que establece que toda persona tiene derecho a que se respete su vida privada[61].

---

confluencia de estos derechos fundamentales. S. RODOTÁ, "Las lecciones de Wikileaks: nueva transparencia y nueva distribución del poder", J.L. PIÑAR MAÑAS (Dir.), VVAA, *Transparencia, acceso a la información y protección de datos*, Reus, Madrid, 2014, págs. 12 y 17.

[58] *Consumer Privacy Bill of Rights Act of 2015*, publicada el 27.2.2015, https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf (fecha consulta: 12.3.2015).

[59] Ver Capítulo IX.

[60] Convenio de Roma, de 4 de noviembre de 1950, para la Protección de los Derechos Humanos y de las Libertades Fundamentales, firmado por España el 24 de noviembre de 1977 y ratificado el 4 de octubre de

Este derecho no es absoluto y podrá ser limitado por las autoridades públicas si se cumplen los requisitos establecidos en el mismo precepto[62]. Estos requisitos son, esencialmente, que la injerencia en el derecho esté prevista en una ley y que sea una medida que responda a uno de los fines legítimos previstos, en el marco de una sociedad democrática (art. 8.2 CEDH)[63].

Respecto a este derecho a no sufrir injerencias en la vida privada, hay que precisar que ya se había recogido en la Declaración Universal de Derechos Humanos aprobada en 1948[64] y en el Pacto Internacional de Derechos Civiles y Políticos de Naciones Unidas[65]. Todos estos textos surgieron con el fin de contrarrestar las atrocidades sucedidas en las dos guerras mundiales. En este sentido, al igual que el *Watergate* precipitó la aprobación de la *Data Privacy Act* estadounidense, se cita también, como importante acicate para contrarrestar el poder de la tecnología en manos de los gobiernos, la utilización por parte de Hitler de la tecnología informática para identificar a las personas pertenecientes a las minorías que fueron objeto del genocidio en la segunda guerra mundial[66].

1979 (BOE núm. 243 de 10.10.1985). Este Convenio fue elaborado en el seno del Consejo de Europa, organización nacida en 1949 tras la segunda guerra mundial con el objetivo de crear una Europa que garantizase el respeto de los derechos humanos, la democracia y la ley.

[61] Concretamente, el artículo 8 CEDH establece: "1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.". Convenio Europeo de Derechos Humanos, Tribunal europeo de Derechos Humanos, Consejo de Europa, Estrasburgo, versión española no oficial, http://www.echr.coe.int/Documents/Convention_SPA.pdf (fecha consulta: 21.6.2015).

[62] M. ARENAS RAMIRO. *El derecho fundamental a la protección de datos personales en Europa, op. cit.*, pág. 110.

[63]Artículo 8.2 CEDH: "No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás."

[64] Aprobada por Resolución de la Asamblea General de la ONU 217 A(III) del 10 de diciembre de 1948. En su artículo 12 establece: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques." J.L. PIÑAR MAÑAS "Protección de datos: origen, situación actual y retos de futuro", P. LUCAS MURILLO DE LA CUEVA, J.L. PIÑAR MAÑAS, *El derecho a la autodeterminación informativa*, Fundación coloquio jurídico europeo, Madrid, 2009, pág. 85.

[65] Aprobado por la Asamblea General en su resolución 2200 A (XXI), de 16/12/1966. En su artículo 17 establece: "1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.". Hay que tener en cuenta que la Declaración Universal de los Derechos Humanos no tenía carácter vinculante, por lo que fue necesario aprobar este Pacto Internacional de Derechos Civiles y Políticos y el Pacto Internacional de Derechos Económicos, Sociales y Culturales, éste último también aprobado mediante la misma resolución indicada, pactos que si son vinculantes para los Estados firmantes.

[66] M.C. GUERRERO PICÓ, *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2006, pág. 28. Esta tesis también se señala en un

En el seno de estas dos organizaciones, el Consejo de Europa y la Organización de Naciones Unidas y en virtud de los preceptos que pretenden preservar la vida privada de los ciudadanos, se adoptaron sendos textos: el Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (en adelante Convenio 108)[67] y los Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales, aprobados por la Resolución 45/95 de la Asamblea General de Naciones Unidas, de 14 de diciembre de 1990 (Principios rectores ONU).

El principal obligado a respetar el artículo 8 CEDH es el Estado, característica del constitucionalismo posterior a la segunda guerra mundial. Así el artículo 8.2 CEDH se refiere a la autoridad pública como la que potencialmente es susceptible de realizar una injerencia que vulnere el derecho a la vida privada. Ante cualquier demanda interpuesta ante el Tribunal Europeo de Derechos Humanos (TEDH), éste establece, en primer lugar si hay injerencia en el derecho a la vida privada. Si considera que se produce esta injerencia, examina si se cumplen los requisitos mencionados para que la autoridad pueda llevarla a cabo y, en este análisis, tiene en cuenta los principios establecidos en el Convenio 108[68].

Sin embargo, el TEDH ha establecido que los Estados deben adoptar las medidas necesarias para asegurar el respeto de la vida privada, incluso en el ámbito de las relaciones entre particulares[69]. De esta forma, el TEDH ha reconocido un efecto

---

informe de la ONU sobre los Principios rectores para la reglamentación de los ficheros computadorizados de datos personales. La Universidad de las Naciones Unidas recuerda, en este informe, al estudiar el principio de lealtad, que la utilización de tales ficheros no debe perseguir objetivos contrarios a los propósitos y principios de la Carta de las Naciones Unidas. Se indica que, tal fue el caso, por ejemplo, de los nazis, quienes en virtud ficheros específicos, efectuaron redadas que permitieron organizar la deportación masiva de ciudadanos judíos. Informe del Secretario General de la Asamblea General de la ONU A/44/606, de 24 de octubre de 1989, sobre los Principios rectores para la reglamentación de los ficheros computadorizados de datos personales, pág. 12.

[67] Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (BOE núm. 274 de 15.11.1985).

[68] Sentencia del TEDH de 4 de diciembre de 2008, *S. and Marper v. The United Kingdom*, apdos. 103 a 126.

[69] El TEDH ha estimado que el Estado debía indemnizar a la recurrente porque no había sido capaz de adoptar las medidas necesarias para garantizar que un hospital cumpliera con las medidas de seguridad necesarias para proteger su historia clínica. Por tanto, el TEDH considera que el Estado ha incumplido sus obligaciones positivas para asegurar el respeto de la vida privada de la recurrente. Sentencia del TEDH de 17 de octubre de 2008, *I v. Finland*, apdo. 47.

horizontal indirecto o *Drittwirkung* del CEDH, de forma que si el Estado no cumple con esas obligaciones positivas, podrá ser condenado como consecuencia de una lesión causada a un particular por otro particular[70].

Si bien el artículo 8.1 CEDH es la primera piedra en la construcción del derecho a la protección de datos, el origen de su regulación en el ámbito europeo se sitúa en la Recomendación (68) 509, de 31 de enero de 1968, sobre los derechos humanos y los nuevos logros científicos y técnicos[71] de la Asamblea parlamentaria del Consejo de Europa. En ella se alertaba sobre el peligro que las nuevas tecnologías (citaba concretamente la interceptación de las comunicaciones telefónicas o las escuchas, la vigilancia, el uso ilegítimo de los estudios estadísticos o similares para obtener información privada, la publicidad subliminal) podían suponer para los derechos y libertades de los individuos y, en concreto, para el derecho reconocido por el artículo 8.1 CEDH. El riesgo detectado aumentaba cuando los Estados miembros no contaban con la legislación necesaria para proteger estos derechos.

Ante la intención manifestada por algunos de los Estados miembros, durante el proceso de redacción de la resolución, de revisar su legislación para incluir mecanismos de protección, la resolución subrayaba la importancia de adelantarse a este paso, con el fin de lograr una mejor armonización de estas regulaciones. Para ello, la resolución recomendaba la realización de un estudio para ver si las legislaciones de los Estados miembros protegían suficientemente el derecho frente al uso de las técnicas informáticas.

Como el resultado de este estudio fue que la protección no era suficiente se dictaron dos resoluciones: la Resolución (73) 22, de 26 de septiembre de 1973, del Comité de Ministros del Consejo de Europa, relativa a la protección de la vida privada de las personas físicas con respecto a los bancos de datos electrónicos en el sector privado y la Resolución (74) 29, de 20 de septiembre de 1974, del Comité de Ministros del Consejo de Europa, referente a la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector público.

[70] L. REBOLLO DELGADO, *Vida privada y protección de datos en la Unión Europea*, Dykinson, Madrid, 2008, págs. 78 a 80.Ver Capítulo VII.
[71] DAVARA RODRÍGUEZ indica que se trata del primer germen legislativo de lo que más tarde se conocería como protección de datos de carácter personal, *La Protección de datos en Europa: principios, derechos y procedimiento*, Grupo Asnef- Equifax, Madrid, 1998, pág. 29.

En estas resoluciones no aparecía expresamente la noción de responsable del fichero, pero sí de manera implícita, ya que el destinatario final de la normativa que los Estados miembros debían adoptar eran las entidades del sector privado o público que gestionaban los bancos electrónicos. En la determinación del ámbito de aplicación de la resolución lo que primaba era el banco electrónico de datos y los datos personales, sea quien fuera quien los utilizara. Por esta razón, se incluyeron definiciones de estos dos conceptos y, sin embargo, no se definió lo que se entendía por sector público o por sector privado.

Los principios se enunciaron de forma neutra, sin indicar quién debía cumplir con los mismos exactamente. Sólo se hacía referencia a obligaciones que debería adoptar el sector público o privado y que repercutirían en las personas que efectivamente operasen con los bancos[72]. De hecho, durante el proceso de elaboración de la Resolución 73 (22) se sugiere la incorporación de la necesidad de designar una persona física que se responsabilizara de los datos[73]. Por tanto, en este primer estadio ya asistimos a un intento de personalización de la responsabilidad. Sin embargo, finalmente se elimina cualquier referencia a esta determinación de la responsabilidad, lo que parece lógico debido a la naturaleza general de este listado de principios[74].

[72] En concreto en la Resolución (73) 22 se establece en su principio 9 que el acceso a la información sólo podrá llevarse a cabo si la persona que accede tiene una razón válida para ello (el conocido como principio del *need to know*). También se establece el hecho de que el personal que opera con los bancos electrónicos (*operating staff of electronic data banks*) debe estar obligado a cumplir con reglas de conducta que prevengan la mala utilización de los datos, concretamente por reglas de secreto profesional. En similares términos se incluyen estas obligaciones en la Resolución (74) 29 en sus principios 6 y 7.

[73] En las observaciones que realizó Francia durante la elaboración de este primer texto dirigido al sector privado se comentó la propuesta realizada por el *Director of Legal Affairs* del *Sub-Committee of the European Committee on Legal Co-Operation*, relativa a la designación de personas físicas que se hicieran responsables de los datos almacenados en los bancos. La delegación francesa propuso un texto en el que se establecía que la responsabilidad del cumplimiento de los principios establecidos en la resolución sería de los directores de la empresa que almacene los datos, a no ser que éstos pudiesen probar que habían delegado poderes en un empleado para asegurar la vigilancia necesaria (En el texto original el texto en inglés es el siguiente: "*responsability for compliance with the rules laid down in this resolution shall lie with the directors of the firm storing the data, unless they can prove that they have conferred effective powers on an employee to ensure the necessary vigilance*"). *Observations by the French authorities on the draft Resolution, Sub-Committee of the European Committee on Legal Co-Operation charged with examining a draft resolution on the protection of privacy vis-a-vis Electronic data Banks in the private sector, CCJ/SC. Prot. Priv. (73)2, Strasbourg, 28 February 1973*, pág. 5.

[74] Así lo entendió la delegación danesa. *Observations by the Danish authorities, Sub-Committee of the European Committee on Legal Co-Operation charged with examining a draft resolution on the protection of privacy vis-a-vis Electronic data Banks in the private sector, CCJ/SC. Prot. Priv.* (*73)3, Strasbourg, 15 March 1973*, pág. 2.

Ambas resoluciones respondieron al deseo de conseguir, de la forma más rápida posible, unos principios básicos para asegurar una protección armonizada en los Estados miembros de la vida privada de los ciudadanos con respecto a los bancos electrónicos de datos. Además, la resolución que primero se aprobó fue la que se dirigía al sector privado, ya que, incluso en ese entonces, se consideró que era el que más riesgos conllevaba.

También hay que resaltar esa primera tendencia a separar la regulación según su destinatario era el sector privado o el público pese a que alguna delegación de los Estados miembros que contribuyeron a la elaboración de los textos no entendía que debiera realizarse esta diferenciación[75]. Para acelerar su aprobación se debieron adoptar estos textos que no son más que meras recomendaciones a los Estados. Sin embargo, lo que se ambicionaba era lograr un instrumento de mayor envergadura en forma de acuerdo internacional que incorporara una regulación vinculante y completa. Este acuerdo sería el Convenio 108, convenio que sí fue un importante paso al introducir en un contexto internacional la noción de responsable. No obstante, antes ya se había introducido la noción en algunas de las primeras leyes que regularon el derecho a la protección de datos en Europa y que, por ello, merecen la atención que a continuación se les brinda.

2. LA APARICIÓN DEL CONCEPTO Y SU INCLUSIÓN EN INSTRUMENTOS INTERNACIONALES

2.1. La aparición del concepto de responsable en la primera generación de leyes de los países europeos de protección de datos: análisis inicial

La primera ley sobre protección de datos que se aprobó en Europa fue una ley regional: la Ley del *Land* alemán de Hesse de 1970. A escala nacional, la primera generación de leyes aprobadas en la materia antes de la aprobación del Convenio 108 fueron la Ley de Suecia, de 11 de mayo de 1973 (*Data Lag 1973:289*); la Ley Federal Alemana, de 27 de enero de 1977 *(Bundesdatenschutzgesetz*, BDGS); la Ley de Francia, de 6 de enero de 1978 (*Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux*

[75] En las observaciones que realiza Francia también se incluye una referencia a que parecía aceptable que esa resolución se dirigiera sólo al sector privado ya que era el que mayor riesgos conllevaría pero que técnicamente los principios podrían aplicarse a ambos sectores. *Observations by the French authorities on the draft Resolution, Sub-Committee of the European Committee on Legal Co-Operation charged with examining a draft resolution on the protection of privacy vis-a-vis Electronic data Banks in the private sector, CCJ/SC. Prot. Priv. (73)2, Strasbourg, 28 February 1973*, pág. 3.

libertés); las Leyes de Dinamarca de 1978, ya que en este caso fueron dos leyes, la Ley 293 que regulaba, por un lado, los ficheros privados (*Danish Private Registers Etc. Act, nº 293, 8 June 1978*), y la Ley 294 que regulaba los ficheros públicos (*Data Public Authorities' Registers Act, nº 294, 8 June 1978*), ambas de 8 de junio de 1978; la Ley nº 48 de Noruega de 9 de junio de 1978 (*Personal Data Files Act*); la Ley de Austria de 18 de octubre de 1978 (*Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten, Datenschutzgesetz 1978, DSG 1978*) y la Ley de Luxemburgo de 31 de marzo de 1979 (*Loi du 31 mars 1979 réglementant l´utilisation des données nominatives dans les traitements informatiques*)[76].

Esta primera oleada de leyes se caracterizó por el incipiente desarrollo de la informática. Por lo tanto, el objetivo de los legisladores fue crear instrumentos de protección que limitasen la utilización desenfrenada de la informática. Los mecanismos utilizados fueron la exigencia de autorización previa para crear ficheros de datos y la creación de autoridades de control encargadas de supervisar los tratamientos de datos[77].

La aprobación del Convenio 108 daría lugar a la segunda generación de leyes, caracterizadas por la tendencia a la simplificación, el abandono de los mecanismos previos de control y la búsqueda de un equilibrio entre la protección de los derechos y el desarrollo de las nuevas tecnologías[78].

Tras la aprobación de la Directiva 95/46/CE se aprobaron las leyes de tercera generación que, al igual que ésta, persiguieron la consecución de la libre circulación de datos mediante una armonización de la protección de los derechos de los ciudadanos. Estas leyes ya no se focalizan tanto en el uso de la informática sino en la protección frente a la acumulación de datos personales[79].

Ante el proceso de reforma, tanto del Convenio 108, como de la Directiva 95/46/CE, podemos decir que estamos, seguramente, a las puertas de la aprobación subsiguiente de las leyes que bien podrían ser consideradas de cuarta generación y que se

[76] M. ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa, op. cit.*, págs. 473 a 475 y de la misma autora, "La protección de datos personales en los países de la Unión Europea", *Revista jurídica de Castilla y León*, nº 16 septiembre 2008, págs. 134 a 163.
[77] *Ibídem.*
[78] *Ibídem.*
[79] *Ibídem.*

caracterizarán por una nueva evolución, fruto una vez más del desarrollo de la tecnología y de la omnipresencia de Internet en nuestras vidas.

La definición de responsable apareció en esa primera generación. Se analizarán las leyes de los Estados miembros de la UE, en las que se incluyó este concepto, es decir, las Leyes de: Suecia, Alemania, Luxemburgo y Austria[80]. También se mencionará la Ley de Francia ya que, pese a no introducir la definición de forma expresa, sí lo hace de forma implícita en su regulación.

Mediante este análisis se quiere iniciar la senda hacia la consecución de uno de los objetivos de este trabajo, que es proponer una metodología para la determinación del sujeto responsable. Para ello, se parte de la disección de la definición incluida en la normativa en diversos elementos que nos puedan ayudar a delimitar los rasgos que caracterizarán a esta figura. Esta división en elementos se ha inspirado en las aportaciones de GRIMALT SERVERA y el GA29, al respecto[81].

La Ley de Suecia define al "responsable del fichero" como: "cualquier persona que mantiene un fichero con el fin de llevar a cabo sus actividades estando el fichero bajo su control"[82]. En esta definición se encuentran ya los principales elementos que distinguiré: el subjetivo, el objetivo y el funcional.

El primer elemento subjetivo nos indicará la naturaleza del sujeto responsable, es decir, qué tipo de sujeto puede incluirse en la misma. En el caso de la Ley de Suecia sería: "cualquier persona". El tipo de persona no quedaba prefijado, ni se limitaba al sector privado o público. El segundo elemento sería el objetivo, es decir, el objeto material sobre

[80] Por tanto, no se hará mención de las Leyes danesas, ya que éstas no contenían ningún concepto de responsable, sino que sólo aludían en su regulación a las empresas o autoridades que mantenían los ficheros. Tampoco se hace referencia a la Ley de Noruega por no ser miembro de la Unión Europea ni formar parte en aquel entonces del Espacio Económico Europeo.

[81] Si bien GRIMALT SERVERA identifica en el análisis que realiza de la figura del responsable del fichero tres elementos: el elemento objetivo, que se refiere al fichero y tratamiento de datos; el elemento subjetivo que es el poder de decisión y el elemento formal que sería la inscripción en el Registro General de Protección de Datos, P. GRIMALT SERVERA, *La responsabilidad civil en el tratamiento automatizado de datos personales, op. cit.*, págs. 44 a 101. El GA29 realiza un análisis mediante la división de la definición de responsable del tratamiento, incluida en la Directiva 95/46/CE en diversos elementos que corresponden a las diferentes partes de la misma. Ver Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.*, y Capítulo II.

[82] Traducción de la autora de la definición de la versión inglesa no oficial de la ley que reza en su Sección 1: "*file controller means any person for the purposes of whose activities a personal data file is kept, where the file is under his control*".

el que el sujeto actuará que, en este caso, es “el fichero”. El fichero será un elemento que vendrá también normalmente definido, al conformar también el ámbito de aplicación, al igual que el dato personal que se incluirá en este fichero. El tercer elemento sería la conducta del sujeto respecto al objeto o lo que calificaré como elemento funcional. Este tercer elemento es el que caracteriza de forma particular al sujeto y lo diferencia respecto a otras figuras. En la ley sueca, se incluyen, por un lado, el mantenimiento (del fichero) y, por otro lado, la exigencia de que el sujeto tenga el control (sobre ese fichero). El hecho de que mantenga el fichero apunta a que este sujeto está activamente ligado al fichero, sería, por lo tanto, un tratador efectivo de los datos que componen el fichero. El poder de control sobre el fichero exige que el sujeto tenga capacidad de decidir sobre este fichero.

Por último, el hecho de que la definición indique que el mantenimiento del fichero se realizará “con el fin de llevar a cabo sus actividades” se refiere a otro aspecto ajeno a los elementos enunciados: la legitimación. Es decir, es una limitación al responsable que sólo podrá mantener el fichero, es decir, utilizarlo, poseerlo, si ello es necesario para que lleve a cabo sus actividades. Esta limitación puede contemplarse también como un derecho o facultad del responsable de tratar los datos, en la medida en que respete la legislación que regula la protección de estos datos.

En conclusión, esta primera definición describe como responsable a un sujeto que utiliza el fichero, lo mantiene y es, por tanto, el tratador efectivo de los datos pero que, además, tiene el control sobre el mismo. Como se verá, estos aspectos evolucionarán y madurarán, adaptándose a la práctica. De esta forma no siempre el tratador efectivo que manipula los datos directamente tendrá el control sobre el fichero, sino que podrán existir diversos personajes alrededor del fichero que carezcan de ese poder.

Tras la ley sueca, se aprobaría la Ley Federal alemana que definiría al “organismo almacenante” como “toda persona o entidad […] que almacene datos para ella misma o los haga almacenar por otros”. Respecto al elemento subjetivo, este “organismo almacenante” se definiría como “toda persona o entidad”. En cuanto al elemento objetivo sobre el que recae la acción del responsable, serían los “datos”. El elemento funcional es el “almacenamiento” y, de nuevo, hallamos la diferenciación entre dos posibles situaciones: que el organismo almacene los datos directamente o que haga que “otros” los

almacenen. Por tanto, el sujeto responsable puede ser el tratador efectivo de los datos o quien pueda decidir que sean otros quienes lleven a cabo la conducta de almacenamiento.

La Ley de Luxemburgo conceptuó al "propietario del banco de datos" como "la persona por cuya cuenta se lleva el banco y que dispone de éste". El elemento subjetivo sería la "persona", el objetivo, el "banco" y el funcional, la "llevanza" o "disposición". De nuevo, se matiza que este propietario del banco de datos dispondrá del mismo, lo que enlaza con la visión del tratador efectivo y también que podrá encomendar la llevanza del banco, lo que alude a la intervención de terceros y a su poder para llevar a cabo esta encomienda.

La Ley austríaca define al "gestor de datos" como "todo titular de derechos o todo órgano o corporación que, por sí mismo o mediante operadores informáticos, tratare datos por medios electrónicos". La identificación de los elementos sería: el subjetivo, que se definiría como el "titular de derechos o todo órgano o corporación", el objetivo, que sería el "banco" y el funcional, que sería el "tratamiento por medios electrónicos". Asimismo, en esta ley también se diferencia claramente que el tratamiento podrá ser realizado por el mismo gestor de datos o mediante operadores informáticos. En este caso, se delimita, no obstante, la naturaleza de quienes actuarán por cuenta del gestor ya que se focaliza en los operadores informáticos.

En la Ley francesa, como se ha indicado, no se incluía ninguna definición del responsable. Sin embargo, en su regulación se establecía como una formalidad previa a poder realizar un tratamiento de datos la notificación o solicitud de informe a la autoridad de control francesa. Uno de los aspectos que debía contener esta notificación o solicitud era la identificación de la persona que presentaba la solicitud y aquella que tenía poder de decidir la creación del tratamiento[83]. A raíz de esta previsión, un tribunal penal estableció que el declarante podría ser toda persona física o jurídica que tuviera poder de decidir la creación del fichero informático aunque encargara la explotación del mismo[84]. La

[83] Así lo establecía el artículo 19 de esta Ley francesa de 1978 que se reproduce: "*La demande d'avis ou la déclaration doit préciser: la personne qui présente la demande et celle qui a pouvoir de décider la création du traitement ou, si elle réside à l'étranger, son représentant en France*".

[84] Pese a que la Ley francesa se refiere al tratamiento de datos, el Tribunal hizo referencia al fichero informático, para definir al responsable como el que decide sobre la creación de este fichero, aunque luego decida subcontratar a alguien para llevar a cabo el tratamiento. Sentencia del *Tribunal correctionel de*

autoridad de control francesa interpretó que el responsable es quien tiene el poder de definir o controlar el contenido y la estructura de este fichero[85].

Asimismo, esta Ley francesa establecía la obligación de preservar la seguridad y la asignaba a "toda persona que ordene o lleve a cabo un tratamiento de informaciones nominativas"[86]. Por tanto, al lado del sujeto con capacidad de ordenar, ya se establece la posibilidad de que exista otro sujeto que será el que lleve a cabo el tratamiento, el tratador efectivo de los datos[87].

Como se puede ver, todas las leyes, a excepción de la Ley de Suecia, se refieren, tanto a la situación en la que el responsable trate los datos por sí mismo, como a la situación en la que otro los trate en su nombre[88]. El hecho de que se establezca la posibilidad de que el responsable pueda utilizar un tercero para realizar la conducta sobre el objeto, lo que deja traslucir, en definitiva, es que tiene el control sobre ese objeto. Es ese poder de control el que le brinda esa capacidad para ordenar a un tercero que le almacene, le lleve o le trate por medios electrónicos el fichero, los datos, el banco o le realice el tratamiento.

La alusión al poder de decisión, de control sobre el tratamiento perdurará en las definiciones vigentes. Sin embargo, en estas primeras leyes, esta capacidad de decidir sobre el elemento objetivo (fichero, datos, banco o tratamiento) se deduce de forma implícita de este poder de encomendar a terceros ciertos usos. Esto cambiará en las leyes actuales para terminar por establecer de forma explícita como elemento funcional el poder de control o de decisión sobre el elemento objetivo, al igual que se refleja ya en la Ley de

---

Versailles, 23 septembre 1986, citado en M.L. LAFFAIRE, *Protection des données à caractère personnel*, Éditions d'Organisation, Paris, France, 2005, pág. 83.

[85] *Ibídem*, pág. 84.

[86] Traducción de la autora del primer apartado del artículo 29 de esta Ley francesa de 1978 que se reproduce: "*Toute personne ordonnant ou effectuant un traitement d'informations nominatives s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou comuniquées à des tiers non autorisés*."

[87] Esta concepción del deber de seguridad como obligación del responsable y quien por su cuenta realice el tratamiento es la que actualmente podemos encontrar en la Directiva 95/46/CE y la normativa que la transpone. Como se verá en los Capítulos IV y V, el deber de seguridad deben cumplirlo los responsables y los encargados del tratamiento. Los encargados del tratamiento serían los tratadores efectivos de los datos que actúan por cuenta de los responsables.

[88] A esta conclusión llega P. GRIMALT SERVERA, que recoge estas primeras definiciones en *La responsabilidad civil en el tratamiento automatizado de datos personales, op. cit.*, págs. 41 a 42.

Suecia, que considera como elemento funcional, el mantenimiento o el control del fichero.

Hay que recalcar la coincidencia de los diversos legisladores, que estimaron pertinente establecer esta noción, con la salvedad de la Ley francesa y las Leyes danesas, con la intención de determinar de alguna forma el sujeto obligado a cumplir lo establecido en esas leyes. Se contrapone, por lo tanto, esta técnica a la que ya se ha visto anteriormente en los EEUU donde se regula con el fin de limitar al poder público o a colectivos concretos del sector privado.

Pese a esa coincidencia en el establecimiento de una definición, del somero análisis realizado de sólo cinco leyes, queda patente también la posibilidad de divergencia en las regulaciones. De un concepto en el que principalmente se manejan tres o cuatro elementos definitorios (por otra parte bastante lógicos) se aprecia una terminología diferente. Esto da una idea de los esfuerzos seguidos a nivel internacional y europeo por armonizar las diferentes regulaciones.

2.2. La inclusión del concepto en los instrumentos internacionales que regulan la protección de datos

2.2.1. El Convenio nº 108 del Consejo de Europa

El Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, es el único instrumento universal vinculante en materia de protección de datos[89]. Sus principios se incluyen en otros instrumentos internacionales como son los Principios rectores ONU[90], y

[89] El Convenio 108 se abrió para su firma a los Estados miembros del Consejo de Europa y para su accesión a los Estados no miembros. El 28 de diciembre de 2014 habían firmado 45 Estados miembros del Consejo de Europa y Uruguay, Estado no miembro había accedido, por lo que para 46 Estados había entrado en vigor el convenio. Turquía pese a firmar el 28 de enero de 1981 no llegó a ratificarlo. España lo firmó el 28 de enero de 1982, lo ratificó el 31 de enero de 1984 y entró en vigor el 1 de octubre de 1985. El Comité de Ministros adoptó el 15 de junio de 1999 una modificación del Convenio 108 con el fin de permitir el acceso por parte de la Comunidad Europea. También hay que tener en cuenta el protocolo adicional que se abrió a la firma el 8 de noviembre de 2001 y entró en vigor el 1 de julio de 2004. Este protocolo versaba sobre las autoridades de control y las transferencias internacionales de datos (*Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data, regarding supervisory authorities and transborder data flows CETS No.: 108*).

[90] En estos principios no se incluyen definiciones sino que es una enumeración de principios inspiradores obtenidos del estudio de las iniciativas existentes en ese momento, aunque se mencionan las "personas encargadas de la creación de un fichero o de su funcionamiento" como obligadas a asegurar el principio de

la Guía OCDE 1980, instrumentos que, no obstante, carecen de la relevancia del Convenio al no ser vinculantes para las partes[91].

Esta norma no tiene carácter *self-executing,* ya que se dirige a los Estados miembros, que son los que deben adoptar las medidas establecidas en el mismo. Por lo tanto, ni los ciudadanos pueden deducir derechos directamente del Convenio[92] ni los responsables tienen obligaciones que deriven del texto[93].

El Convenio busca un equilibrio, entre el poder que el uso de la información mediante la informática brinda a los sectores público y privado, y la protección de las personas frente a dicho uso. Los responsables deberán asegurarse de que las ventajas que les proporciona el tratamiento de la información no conlleven el debilitamiento de la posición de las personas cuyos datos se utilizan[94]. En consonancia con esta idea de hacer

---

calidad. También se alude a las "personas u organismos responsables del procesamiento de los datos o de su aplicación" cuando se establece que la autoridad encargada de controlar los principios establecidos debe ser independiente e imparcial respecto a estas personas (apdos. A, 1 y 8 Principios rectores ONU).

[91] Resolución del Consejo de Europa Nº 3 sobre protección de datos y privacidad en el tercer milenio, adoptada el 26 de noviembre de 2010, apartado 10 que recuerda que el Convenio 108 es el único instrumento vinculante en el ámbito de la protección de datos y cuyos principios básicos se encuentran incorporados en otros instrumentos internacionales como los mencionados de la ONU y de la OCDE. *Data protection compilation of Council of Europe texts, Directorate General of Human Rights and Legal Affairs, Council of Europe, Strasbourg, November 2010*, www.coe.int/t/dghl/standardsetting/dataprotection/dataprotcompil_en.pdf (fecha consulta: 8.1.2015).

[92] *Data protection compilation of Council of Europe texts, op. cit.*, *Explanatory report Convention for the protection of individuals with regard to automatic processing of personal data*, apdo. 38. No obstante, hay que destacar que pese a que no se pueda aplicar directamente sí ha servido para que, en el caso de España, nuestro TC haya interpretado el artículo 18.4 CE a la luz de este texto vía el artículo 10.2 CE, cuando aún no se había desarrollado legalmente el mismo. Así, en la STC 254/1993 se resolvió un recurso de amparo contra la denegación en el año 1986 por parte del Gobernador Civil de Guipúzcoa y del Ministerio de Interior de la comunicación de la información que había solicitado el recurrente acerca de si la Administración del Estado disponía de ficheros automatizados donde figuraran sus datos, la información de la finalidad de esos ficheros y de la autoridad que los controlaba y los datos en concreto incluidos en estos ficheros. En ese momento no existía normativa sobre protección de datos, ya que aún no se había aprobado la LORTAD en 1992. Por ello, el recurrente había fundado su solicitud en el Convenio 108 que entró en vigor para España el 1 de octubre de 1985 y concretamente en el artículo 8 de este Convenio 108. El TC considera que, en virtud del artículo 10.2 CE, los textos internacionales pueden desplegar ciertos efectos respecto a los derechos fundamentales, "en cuanto pueden servir para configurar el sentido y el alcance de los derechos recogidos en nuestra Constitución" (FJ 6).

[93] A. TÉLLEZ AGUILERA. *La Protección de datos en la Unión Europea: divergencias normativas y anhelos unificadores, op. cit.*, pág. 42.

[94] Así lo indica el Informe explicativo del Convenio 108 que reza exactamente: ""*Information power" brings with it a corresponding social responsibility of the data users in the private and public sector. In modern society, many decisions affecting individuals are based on information stored in computerised data files: payroll, social security records, medical files, etc. It is essential that those responsible for these files should make sure that the undeniable advantages they can obtain from automatic data processing do not at the same time lead to a weakening of the position of the persons on whom data are stored*." *Data protection compilation of Council of Europe texts, op. cit.*, *Explanatory report Convention for the protection of individuals with regard to automatic processing of personal data*, pág. 19.

responsables a quienes se benefician de la informática, el texto introduce el concepto de "autoridad controladora del fichero"[95]. Como señalara Vittorio Frosini, la inclusión de este concepto reviste una gran importancia para la cuestión de la responsabilidad, ya que establece que el gestor del banco de datos será una persona física o jurídica, que, por lo tanto, será responsable civil y penalmente[96].

La autoridad controladora del fichero se define como "la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán" (art. 2.d) Convenio 108).

Si aplicamos el análisis iniciado con las leyes nacionales europeas, en cuanto al elemento subjetivo, podrá ser considerada autoridad controladora del fichero una persona física o jurídica, supuestos que parecen apuntar a cualquier sujeto que pueda operar en el sector privado. Por otro lado, se señala a una autoridad pública, servicio o cualquier otro organismo, figuras que claramente apuntan al sector público. El Convenio 108 contiene, por tanto, una regulación común a estos dos sectores (art. 3.1 Convenio 108). No obstante, se deja abierta la posibilidad de modular el ámbito de aplicación del Convenio 108, de forma que los Estados podrían extraer del mismo a determinados ficheros, siempre que no estuvieran ya sometidos a normativa interna en materia de protección de datos (art. 3.2.a Convenio 108)[97].

En cuanto al elemento objetivo la definición se refiere al fichero automatizado y a los datos de carácter personal. Por el momento, no aparece la noción de tratamiento que posteriormente adquirirá relevancia en la delimitación del objeto. Se centra en este momento el ámbito material en el fichero automatizado y en los datos relativos a personas físicas. No obstante, el Convenio 108 permite a los Estados parte ampliar la aplicación del mismo respecto a datos relativos personas jurídicas y a ficheros manuales (art. 3.2.b y c Convenio 108).

---

[95] Una traducción algo desafortunada de la versión en francés "*maître du fichier*" y la versión en inglés "*data controller*".

[96] V. FROSINI, "La Convenzione Europea sulla protezione dei dati", *Revista di diritto Europeo, Anno XXIV n.1 Gennaio-Marzo* 1984, pág. 14.

[97] *Data protection compilation of Council of Europe texts, op. cit., Explanatory report Convention for the protection of individuals with regard to automatic processing of personal data*, págs. 22 a 23.

El elemento funcional es la decisión: "que sea competente con arreglo a la ley nacional para decidir"[98]. La determinación de quién es competente para decidir se efectuará al acudir a la ley nacional que lo establezca. Esta característica, propia de una norma internacional, parecería que remite a las leyes nacionales que puedan regular la actividad del sujeto responsable, de forma que si esa actividad conlleva que tenga que decidir sobre los aspectos incluidos en la definición (finalidad, categorías de datos y operaciones) debería considerarse responsable[99].

Sin embargo, llama la atención que el Informe explicativo del Convenio 108 indique que la referencia a la ley nacional tiene en cuenta que las leyes nacionales de protección de datos ya establecen los criterios específicos para determinar quién será la persona competente para decidir[100]. Parece, por tanto, una remisión a los conceptos que se establecen en las leyes nacionales de protección de datos de los Estados parte pero, entonces ¿Para qué incluir un concepto en el Convenio 108? En todo caso, este reenvío ya permite entrever la dificultad de la aplicación práctica del concepto.

En el concepto del Convenio 108, en referencia a las leyes nacionales europeas estudiadas, se especifican con más detalle los aspectos concretos del elemento objetivo sobre los que el responsable decide. De esta forma, el responsable decidirá sobre la finalidad del fichero automatizado, las categorías de datos de carácter personal que deberán registrarse y las operaciones que se llevarán a cabo. Por tanto y, sin perjuicio de la remisión comentada a las leyes nacionales de protección de datos, si el sujeto tiene la capacidad de decidir sobre estas cuestiones será considerado responsable. En este sentido, cabe resaltar que no se incluyen aspectos tan esenciales como los destinatarios de los datos.

---

[98] El subrayado es de la autora.

[99] De hecho esta remisión a la normativa nacional no estaba en el borrador anteriormente referenciado en el que la definición sólo se refería a la capacidad de decidir: *""controller of the file" means the natural or legal person, public authority, agency or any other body which is competent to decide which categories of personal data should be recorded and which processes should be applied to them". Draft Convention for the protection of individuals with regard to automated data files prepared by the Secretariat following the meeting of Working Party No. 1 of the Committee of Experts on Data Protection (CJ-PD-GT1) held in Strasbourg from 16 to 18 January 1979, Council of Europe, CJ-PD-GT1 (79)1, Strasbourg, 19 January 1979*, pág. 2.

[100] *Data protection compilation of Council of Europe texts, op. cit., Explanatory report Convention for the protection of individuals with regard to automatic processing of personal data,* pág. 22. Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.*, pág. 9.

Por último, indicar que el Informe explicativo del Convenio 108 especifica que el concepto sólo se refiere a la persona que se configura como el responsable último del fichero y no se incluyen los sujetos que puedan llevar a cabo operaciones de acuerdo con las instrucciones de la autoridad controladora del fichero[101]. Por tanto, aclara que no serán responsables quienes actúen por cuenta del mismo.

Pese a la importancia del establecimiento de este concepto, lo cierto es que después no se menciona en el texto más que dos veces la figura. Sin embargo, hay que entender que la incorporación de esta definición implica que las obligaciones que se enuncian de forma neutra deben ser cumplidas por este sujeto.

El Convenio 108 sólo hace referencia a la autoridad controladora del fichero en dos artículos: el 8 y el 14. En el artículo 8.a) del Convenio 108, como parte de la información que se deberá ofrecer al titular de los datos, se incluye "la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero". El objetivo de este precepto es asegurar que el titular de los datos conoce que se lleva a cabo un tratamiento de sus datos. El hecho de saber quién lo lleva a cabo permitirá que el titular pueda dirigirse a esta autoridad y así ejercer las facultades que el Convenio 108 le otorga[102].

El artículo 14 del Convenio 108 se refiere a la asistencia a las personas que residan en el extranjero con el fin de facilitarles el ejercicio de sus derechos. Así, las personas que residan en el territorio de otro Estado parte podrán presentar una demanda a través de la autoridad designada por ese Estado parte y, entre la información que debe

[101] *Data protection compilation of Council of Europe texts, op. cit.*, *Explanatory report Convention for the protection of individuals with regard to automatic processing of personal data*, pág. 22.

[102] El artículo 8 Convenio 108 establece en los siguientes apartados la posibilidad para la persona concernida de "b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible; c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio; d) disponer de un recurso si no se ha atendido a una petición de confirmación, o, si así fuere el caso, de comunicación, de rectificación o de borrado, a que se refieren los párrafos b) y c) del presente artículo." Respecto a lo que indica el apartado c), el artículo 5 se refiere al principio de calidad de los datos y el artículo 6 se refiere a las categorías particulares de datos, es decir, los datos que revelan el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de salud o de vida sexual y de condenas penales.

constar en la petición de asistencia, se exige que se indique el fichero automatizado de datos al que se refiere la demanda o la autoridad controladora del fichero.

Se comprende mejor la importancia que hubiera podido tener el concepto en el texto si acudimos a los documentos preparatorios. Inicialmente se obligaba a los Estados parte a no aceptar que se llevara a cabo un tratamiento de datos personales en sus territorios si no se podía identificar a la autoridad controladora del fichero[103]. Además de la utilidad que para el afectado tiene conocer la identidad y la dirección de la autoridad controladora del fichero, durante la elaboración del Convenio 108 se abordó la cuestión de la determinación de la legislación aplicable[104]. Uno de los criterios que se barajaron para esta determinación de la ley aplicable fue la residencia habitual de la autoridad controladora del fichero[105].

La previsión sobre la ley aplicable se eliminó del texto definitivo, donde no aparece ninguna mención a este posible conflicto. Las delegaciones de expertos que trabajaron en el proyecto se dieron cuenta de que era demasiado pronto para discutir esta

[103] Artículo 3.5 de uno de los primeros borradores del Convenio, *Draft Convention for the protection of individuals with regard to automated data files prepared by the Secretariat following the meeting of Working Party No. 1 of the Committee of Experts on Data Protection (CJ-PD-GT1) held in Strasbourg from 16 to 18 January 1979, Council of Europe, CJ-PD-GT1 (79)1, Strasbourg, 19 January 1979*, pág. 4.

[104] En el borrador referenciado se establecía el artículo 4 dedicado a esta cuestión, *Ibídem*, pág. 5. Asimismo, en los comentarios realizados sobre este borrador por la Secretaría del Comité encargado de preparar el texto del Convenio 108 (el Comité Experto de Protección de Datos) se reflejó el acuerdo de todos los expertos en el texto del artículo 3.5 comentado del borrador, precisamente porque era esencial para poder aplicar el artículo 4. De hecho, se indicaba que algunos Estados como Noruega obligaban al responsable a residir en su territorio y otros como Francia establecían que, si éste no residiera en su territorio designara a un representante. Además se especificaba que no podría ser apto para representar al responsable un "centro de tratamiento" ya que no tenía la capacidad de darse órdenes a si mismo. *Commentaires du Secrétariat au projet révisé de Convention pour la protection des personnes à l'égard des fichiers automatisés, Comité d'experts sur la protection des données, Conseil de l'Europe, CJ-PD-GT1 (79)2, Strasbourg, le 22 janvier 1979*, pág. 4.

[105] Otros criterios fueron el lugar donde se efectuaba el tratamiento y la residencia del afectado, titular de los datos. Sin embargo, la Secretaría del Comité de Expertos de Protección de Datos, al comentar esta cuestión y estudiar la viabilidad de aplicar estos criterios, consideró que el que parecía ser la mejor solución era el criterio de la residencia de la autoridad controladora del fichero. Los motivos que alegaba eran que, en virtud de lo dispuesto por el artículo 3.5 del borrador, ya comentado, se aseguraba la posibilidad de identificar a este responsable. Estimaba que podía ser más fácil establecer mecanismos para que el responsable se ubicara en uno de los Estados contratantes que optar por el lugar del tratamiento, más impreciso y fácilmente modificable, o el lugar de residencia del afectado que conllevaría también dificultades en la aplicación de la resolución adoptada al responsable que pudiera ubicarse en otro país, en virtud de una ley de un país diferente. *Commentaires du Secrétariat au projet révisé de Convention pour la protection des personnes à l'égard des fichiers automatisés, Comité d'experts sur la protection des données, Conseil de l'Europe, CJ-PD-GT1 (79)2, Strasbourg, le 22 janvier 1979*, págs. 5 a 7.

polémica cuestión y que este punto iba a retrasar la aprobación del texto[106]. Por último, hay que mencionar que el Convenio 108 está sumido en un proceso de modernización al que me aproximaré en el último capítulo de esta tesis.

2.2.2. La Guía de la Organización de Cooperación y Desarrollo Económico relativa a la protección de la privacidad y de las transferencias de datos personales

En 1969 la OCDE encargó a un grupo de expertos (el panel de los bancos de datos o *Data Bank Panel*) que analizara diversos aspectos relativos a la privacidad. Los resultados obtenidos fueron: el reconocimiento de que era preciso realizar transferencias de datos entre los diferentes Estados, pero que se debían evitar las mismas si podían conllevar riesgos para la seguridad o el posible incumplimiento de leyes nacionales, el gran valor de la información, la necesidad de medidas de seguridad y del compromiso de los países para establecer una serie de principios para proteger la información personal.

Como consecuencia de estos primeros resultados, en 1978 la OCDE encargó a un nuevo grupo de expertos el desarrollo de una guía que incluyera unos principios básicos para regular las transferencias de datos para asegurar una armonización en las legislaciones nacionales de los Estados parte. Estos trabajos se realizaron conjuntamente con el Consejo de Europa y con la Comisión Europea y dieron como resultado la Guía OCDE 1980 que no tiene carácter vinculante[107].

---

[106] Esta decisión se plasmó en el Informe explicativo de la Convención 108 que explica que el comité de expertos, encargado de su elaboración, se había planteado la cuestión de la ley aplicable. El comité finalmente había decidido que era prematuro incluir en la Convención reglas específicas sobre este tema. No obstante, se indicaba que el problema de la ley aplicable se mantendría pendiente de que en un momento posterior se abordara si fuera preciso mediante un Protocolo a la Convención, protocolo que nunca llegó a elaborarse. *Data protection compilation of Council of Europe texts, op. cit.*, *Explanatory report Convention for the protection of individuals with regard to automatic processing of personal data,* pág. 22. De hecho, la sugerencia de incluir un protocolo adicional vino de los expertos españoles que lo propusieron con el ánimo de acelerar el acuerdo y de que el tema se analizara por especialistas en derecho internacional privado. Las expertos argumentaron que la Convención sólo incluía unos principios básicos y la disposición que se quería incluir sobre ley aplicable necesariamente iba a tener naturaleza *self-executing*, lo que podía suponer una mayor resistencia por parte de los parlamentos a su aprobación, al implicar la no aplicación en esta materia de las reglas de conflicto establecidas en los ordenamientos nacionales. *Draft Convention for the protection of individuals with regard to automated data files (CJ-PD-GTI (79)1), Committee of experts on data protection, Working Group No. 1, Comments of the Spanish experts, CJ-PD-GT1 (79)5, Strasbourg, 22 March 1979*, págs.1 a 2.

[107] *Explanatory memorandum. OECD Guidelines on the protection of privacy and transborder flows of personal data*. http://www.oecd.org/Internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (fecha consulta: 21.7.2014).

En 2013 se actualizó la Guía de la OCDE, con el fin de adaptarla a los nuevos riesgos para la privacidad que acarrearon los avances tecnológicos[108]. Entre los principales aspectos tratados durante la revisión de la guía estuvo el de los roles y responsabilidades de los actores clave y la aplicación proactiva de los principios[109]. Entre los cambios que se llevaron a cabo estuvo el desarrollo del principio de *accountability*, que ya se encontraba en la versión de 1980. Este principio, que se ha traducido como de responsabilidad o de rendición de cuentas, obliga al responsable a adoptar las medidas que aseguren el cumplimiento de los principios de la guía[110].

Sin embargo, en el enfoque seguido en este proceso de cambio se optó por actualizar la guía mediante modificaciones más bien sutiles y no por una reforma a fondo de los principios[111]. Así, en la nueva versión de la Guía OCDE 2013 se mantiene intacto el concepto de responsable, pero el grupo de expertos encargado de llevar a cabo la revisión (encabezado por Jennifer Stoddart, *Privacy Commissioner of Canada*) señaló su revisión como un aspecto que debía tenerse en cuenta en futuras reformas[112]. Así, el grupo planteó, como cuestión pendiente de analizar, si esta definición debía actualizarse para tener en cuenta el aumento de la diversificación y de la colaboración entre organizaciones en el uso de los datos. El grupo también dejó para futuros estudios otra importante cuestión: si deberían reflejarse en las regulaciones del derecho de protección de datos otros roles de actores diferentes a los responsables como, por ejemplo, los desarrolladores de sistemas informáticos.

---

[108] *Recommendation of the Council concerning Guidelines governing the protection of privacy and transborder flows of personal data (2013), C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79.* http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (fecha consulta: 21.7.2014). Como indicó Michael Kirby, quien lideró la elaboración de la Guía OCDE 1980, en la celebración del 30 aniversario de la misma: "*In the field of information policy, the technology is such that no international expression of principles can be immune from the forces of change*". *Remarks from Hon. Michael Kirby on the 30th anniversary of the OECD, Privacy Guidelines*, www.oecd.org/Internet/Interneteconomy/49710223.pdf.

[109] *Recommendation of the Council concerning Guidelines governing the protection of privacy and transborder flows of personal data (2013), C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79. Suplementary explanatory memorandum.*

[110] Ver Capítulo IX.

[111] O. TENE, "Reforming data protection in Europe and beyond", A. RALLO LOMBARTE, R. GARCÍA MAHAMUT (Ed.), VVAA, *Hacia un nuevo derecho europeo de protección de datos. Towards a new European data protection regime*, Tirant lo Blanch, Valencia, 2015, pág. 162.

[112] OECD (2013), "*Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines*", *OECD Digital Economy Papers, No. 229, OECD Publishing*, págs. 6, 11. http://dx.doi.org/10.1787/5k3xz5zmj2mx-en (fecha consulta: 8.8.2014).

La definición de responsable de los datos (*data controller*) establecida en la Guía OCDE 2013 es aquella "parte que, de acuerdo con la ley nacional, es competente para decidir sobre el contenido y uso de los datos personales, sin tener en cuenta si los datos se recogen, almacenan, tratan o se comunican por esta parte o por un agente en su nombre"[113].

Si realizamos el análisis del concepto, respecto al elemento subjetivo se proporciona menos detalle acerca de la determinación de quién podrá considerarse responsable ya que, si en el Convenio 108 se establecía que podía ser una persona física o jurídica, autoridad pública, agencia u otra entidad, en la Guía OCDE 2013 sólo se alude a que se trata de una parte (*party*).

El elemento objetivo difiere respecto al Convenio 108. Si en aquel texto se refería al fichero y los datos de carácter personal sin referirse al tratamiento, la Guía OCDE 2013 se refiere a los datos. Ni en la Guía OCDE 1980 ni en la versión revisada en 2013 se incluye la definición de tratamiento, sino sólo de datos personales[114]. Sin embargo, en la última parte de la definición, se alude a varias operaciones, entre las que se menciona al tratamiento (*processed*): "decide sobre el contenido y uso de los datos personales, sin tener en cuenta si los datos se recogen, almacenan, tratan o se comunican por esta parte o por un agente en su nombre". Entre estas operaciones, aparece el concepto "comunicación", en clara coherencia con el objetivo perseguido con esta regulación: facilitar las transferencias internacionales.

Respecto al elemento funcional, en esta definición también se alude a la capacidad de decisión del responsable, como se hacía en el Convenio 108. Asimismo también coinciden ambos instrumentos en el reenvío a la legislación nacional para determinar quién será este responsable que es competente para decidir.

En cuanto a los aspectos concretos del objeto sobre los que decide el responsable es donde más divergencias se suscitan en ambos textos. En el caso del Convenio 108 el

[113] Traducción de la autora: "*data controller" means a party who, according to national law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf*" (punto 1.a Guía OCDE 2013).
[114] Los datos personales se definen, en ambas versiones, como sigue: "*personal data means any information relating to an identified or identifiable individual (data subject)*" (punto 1.b) Guía OCDE 2013).

responsable decide sobre la finalidad del fichero automatizado, qué categorías de datos de carácter personal deberán registrarse y qué operaciones se les aplicarán. En el caso de la Guía OCDE 2013, el responsable decide sobre el contenido y uso de los datos personales, por lo que se obvia la finalidad. Como se verá la finalidad se configurará como el aspecto más importante sobre el que decidirá el responsable. Por ello, resulta importante señalar esta diferencia, aunque se podría entender que, al referirse al uso, podría referirse al fin que se dará a los datos personales, al responder a la pregunta ¿qué se hará con los datos?[115].

En la definición se prevé la posibilidad de que exista un tercero, que realice el tratamiento por cuenta del responsable, el tratador efectivo. Se deja claro, no obstante, que este tercero no se considerará responsable, ya que no decidirá sobre el contenido y uso de los datos.

Las definiciones establecidas en el Convenio 108 y en la Guía OCDE 2013 relativa a la protección de la privacidad y de las transferencias de datos personales constituyen la plasmación a nivel internacional del concepto de responsable. Esta plasmación en el Convenio 108 tiene como objetivo equilibrar la balanza en la que, por un lado, están las ventajas y el poder que supone para estos sujetos responsables la utilización de las tecnologías y, por el otro está la protección de los derechos (especialmente del derecho a la vida privada) de los ciudadanos cuyos datos se utilizan[116].

La Guía OCDE 2013 no responde a la defensa de los derechos humanos, sino a la defensa del desarrollo económico que ve como una traba a éste la existencia (o inexistencia) de regulaciones divergentes que protejan los datos[117]. Sin embargo, este texto ha bebido de la regulación del Convenio 108, por lo que es lógico que también haya incorporado la definición de responsable. Al igual que en el Convenio 108, la definición

[115] Como se verá en la legislación española estos aspectos concretos sobre los que decidirá el responsable serán la finalidad, contenido y uso del tratamiento. En la Directiva 95/46/CE serán los fines y los medios del tratamiento.

[116] Así lo indica el artículo 1 Convenio 108 que establece el objeto y el fin del texto: "El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona."

[117] Hay que tener en cuenta que no es el objetivo primordial de esta organización la protección de los derechos humanos, a diferencia del Consejo de Europa, con el Convenio Europeo de Derechos Humanos de 1950, del que deriva el Convenio 108.

no tiene un papel decisivo en la regulación. La utilización de la misma permite identificar a los sujetos que finalmente deberán aplicar las legislaciones nacionales pero se remite básicamente a las mismas para su determinación.

2.2.3. Asia-Pacific Economic Cooperation Privacy Framework

El foro de cooperación económica de la región Asia-Pacífico (APEC) estableció un sistema no vinculante de cooperación que pretendía incentivar las transferencias de datos entre sus Estados miembros mediante la protección de la privacidad. De nuevo, el objetivo era principalmente económico[118]. Este sistema tiene como base el APEC Privacy Framework, inspirado en la Guía OCDE 1980[119], en el que se establecieron, en noviembre de 2004, nueve principios que debían ayudar a los Estados miembros a desarrollar un enfoque coherente en materia de protección de la privacidad.

Al responsable se le denomina responsable de información personal (*personal information controller*) y se define como "la persona u organización que controla la recogida, el mantenimiento, el tratamiento o uso de información personal. Se incluye la persona u organización que encargue a otra persona u organización la recogida, mantenimiento, tratamiento, uso, transferencia o comunicación de información personal por cuenta suya, pero se excluye la persona u organización que lleve a cabo estas funciones por instrucciones de otra persona u organización. También se excluye al individuo que recoge, mantiene, trata o usa información personal en conexión con asuntos personales, familiares o domésticos del propio individuo"[120].

---

[118] Los objetivos de esta organización son los llamados "Objetivos Bogor", al acordarse en Bogor, Indonesia, en 1994, y consistían en lograr una zona de libre comercio e inversión en el área Asia-Pacífico en 2010 para los países industrializados y en 2020 para los países en vías de desarrollo. Los miembros de APEC son 21 países a los que se denomina "economías miembro", ya que el principal interés de esta organización es la economía (Australia; Brunei Darussalam; Canada; Chile; República Popular de China; Hong Kong, China; Indonesia; Japón; Republica de Corea; Malasia; Mexico; Nueva Zelanda; Papua Nueva Guinea; Peru; República de Filipinas; Federación Rusa; Singapur; Chinese Taipei; Tailandia; Estados Unidos de América; y Vietnam). http://www.apec.org/FAQ.aspx (fecha consulta: 11.8.2014).

[119] APEC Privacy Framework, *APEC#205-SO-01.2, APEC Electronic Commerce Steering Group (ECSG)*, 2005, punto 5 preámbulo. http://publications.apec.org/publication-detail.php?pub_id=390 (fecha consulta: 11.8.2014).

[120] Traducción de la autora de la definición contenida en APEC Privacy Framework, apartado 10, que se reproduce: *"Personal information controller means a person or organization who controls the collection, holding, processing or use of personal information. It includes a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf, but excludes a person or organization who performs such functions as instructed by another person or organization. It also excludes an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs."*

Pese a que el APEC Privacy Framework se inspira en la Guía OCDE 1980, las definiciones de responsable contenidas en ambos instrumentos no son idénticas. El elemento subjetivo es la "persona u organización" y se deja claro que se aplica a ambos sectores público y privado. El elemento objetivo es la "información personal" que se define como "cualquier información sobre un individuo identificado o identificable"[121]. El elemento funcional es la capacidad de "control" sobre la información personal y, en concreto, sobre "la recogida, el mantenimiento, el tratamiento o uso" de la misma.

En esta definición destaca la conexión con la delimitación del ámbito de aplicación, en el que se incluye. Las definiciones juegan un papel delimitador, como se verá, en las leyes de protección de datos y, en concreto, respecto al responsable, habrá que analizar si el sujeto al que se refiere la definición cumple con los requisitos establecidos para poder aplicar la ley o, en este caso el APEC Privacy Framework.

De esa forma, se incluyen en la definición aspectos que habitualmente se encuentran diferenciados y que se suelen incluir en otros conceptos o disposiciones. Así, en vez de incluirse una definición separada de tratamiento de datos, se desglosan en el concepto de responsable, las operaciones concretas sobre las que se extenderá el poder de control del responsable. También, se indica que no será responsable la persona que realice esas operaciones para fines personales, lo que suele formar parte de las exclusiones habituales del ámbito de aplicación de las normas de protección de datos.

Se deja claro, en la definición, que no será considerada responsable la persona u organización que lleve a cabo las operaciones descritas por cuenta de otra persona u organización. Estos aspectos denotan que, en el momento en el que se adoptó el APEC Privacy Framework, el año 2004, ya había Estados miembros de la APEC que contaban con una regulación y una cultura sobre la privacidad consolidadas[122]. Por ello, se aprecia un esfuerzo por diferenciar la figura del responsable de la del prestador que actúa por cuenta del mismo.

[121] Traducción de la autora de la definición contenida en APEC Privacy Framework, apartado 9 que se reproduce: "*Personal Information means any information about an identified or identifiable individual*".
[122] APEC Privacy Framework, apartado 9 (parte explicativa).

2.2.4. La propuesta conjunta para la redacción de estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal de Madrid

Por último, resulta interesante hacer referencia a la Propuesta conjunta para la redacción de estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal (Propuesta de Madrid). Este texto respondió a la idea por parte de las autoridades de control de que era preciso adoptar un enfoque internacional en la regulación del derecho a la protección de datos. La iniciativa fue especialmente impulsada por la Agencia Española de Protección de Datos (AEPD), que presentó el documento en la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, que ella misma organizaba y que tuvo lugar el 5 de noviembre de 2009, en Madrid[123].

Pese a no tener fuerza vinculante, se trata de un documento importante aunque sea a nivel jurídico, ya que aglutina la experiencia de las autoridades de control. Se puede decir que se trata de una especie de desiderátum que las autoridades plasmaron en forma de instrumento. El deseo era alcanzar un nivel de protección universal que hiciera posible contrarrestar los problemas que provocaba la globalidad de los intercambios de información y un mal uso de la tecnología[124]. Asimismo, se quería suplir la disparidad existente en las normativas de los países, así como la carencia en algunos de este tipo de

[123] Las Conferencias Internacionales se iniciaron en Bonn, en 1979. Son un foro de encuentro anual en el que se reúnen autoridades de control de todo el mundo a puerta cerrada pero también se organizan sesiones abiertas en las que participa el sector privado y la sociedad civil. La Conferencia se ha ido dotando con el tiempo de una estructura que asegura una continuidad en los trabajos que se llevan a cabo. http://www.agpd.es/portalwebAGPD/internacional/Conferencias_inter/index-ides-idphp.php (fecha consulta: 29.7.2015). Fueron concretamente la AEPD y la autoridad de control suiza (*Préposé fédéral à la protection des données et à la transparence*) las que propusieron desarrollar este instrumento de carácter universal, en la 30ª Conferencia Internacional de protección de datos y de autoridades de control, que se celebró en el 2008. *Resolution on the urgent need for protecting privacy in a borderless world, and for reaching a Joint Proposal for setting International Standards on Privacy and Personal Data Protection, 30th International Conference of Data Protection and Privacy Commissioners Strasbourg, 17 October 2008*,https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/08-10-17_Strasbourg_international_standards_EN.pdf (fecha consulta: 29.7.2015).

[124] *Resolution on the urgent need for protecting privacy in a borderless world, and for reaching a Joint Proposal for setting International Standards on Privacy and Personal Data Protection, 30th International Conference of Data Protection and Privacy Commissioners Strasbourg, 17 October 2008*, pág. 3. En esta línea DAVARA FERNÁNDEZ proponía también la elaboración de un estándar internacional en I. DAVARA FERNÁNDEZ DE MARCOS, *Hacia la estandarización de la protección de datos personales. Propuesta sobre una "tercera vía o tertium genus" internacional*, La Ley, Las Rozas (Madrid), 2011.

regulación[125]. Para ello, se quería elaborar un documento de naturaleza vinculante, que aunara los principios comunes que yacían en los diversos instrumentos jurídicos internacionales, de forma que se hiciera con la anuencia del máximo de participantes en el proceso[126].

En la definición de su objeto se expresa la dualidad que ya se ha observado en los textos internacionales que se han analizado. Por un lado, se persigue la protección uniforme a nivel internacional de unos principios de protección de los datos y con ello se quiere facilitar los flujos internacionales de datos, necesarios en un mundo globalizado. De esta forma, lo que se pretende es que ningún Estado pueda limitar esta circulación por alegar que no se protegen los datos personales fuera de sus fronteras. Lo que se busca es que todos, titulares de datos y responsables, se beneficien de las ventajas de un instrumento de este nivel[127]. Además, se concibe como una regla de mínimos que los Estados miembros pueden completar, de forma que puedan establecer una protección más reforzada en sus territorios. No obstante, este mínimo permitirá que se puedan realizar transferencias internacionales sin problemas.

El deseo de universalidad se manifiesta en la remisión a la Declaración Universal de Derechos Humanos y al Pacto Internacional de Derechos Civiles y Políticos, como instrumentos que han de guiar el tratamiento leal de datos de carácter personal, contrarios especialmente a los tratamientos de datos que den lugar a una discriminación injusta o arbitraria. En esta línea, se observa también la influencia de los Principios rectores ONU, instrumento que incluye precisamente un principio de no discriminación[128].

[125] *Resolution on the urgent need for protecting privacy in a borderless world, and for reaching a Joint Proposal for setting International Standards on Privacy and Personal Data Protection, 30th International Conference of Data Protection and Privacy Commissioners Strasbourg, 17 October 2008*, pág. 3.
[126] *Ibídem.* A. TRONCOSO REIGADA, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *Revista Española de Derecho Europeo*, núm. 43/2012, Aranzadi, pág. 18.
[127] Así, no sólo las autoridades perseguían este objetivo sino también, como demuestra la declaración de 27 de octubre de 2009, las grandes empresas tecnológicas. http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.1.pdf (fecha consulta: 29.7.2015)
[128] En concreto, se trata del Principio 5 de los Principios rectores ONU que reza así: "A reserva de las excepciones previstas con criterio limitativo en el Principio 6, no deberían registrarse datos que puedan originar una discriminación ilícita o arbitraria, en particular información sobre el origen racial o étnico, color, vida sexual, opiniones políticas, convicciones religiosas, filosóficas o de otro tipo o sobre, la participación en una asociación o la afiliación a un sindicato".

Esta propuesta es el colofón a la evolución de la normativa en esta materia. Y, en definitiva, si bien no se alcanzó este ambicioso objetivo, la Propuesta de Madrid ha servido para promover un proceso de reflexión sobre la regulación que ha sido fuente de inspiración, por ejemplo, en la reforma del Convenio 108[129].

Como ejemplo de esta evolución jurídica, la terminología utilizada en las definiciones denota un esfuerzo por encontrar la neutralidad y la simplificación Así, el responsable se define como "persona responsable: persona física o jurídica, de naturaleza pública o privada que, sola o en compañía de otros, decida sobre el tratamiento" (apdo. 2.d) Propuesta de Madrid).

Como se puede apreciar, en este esfuerzo por simplificar se alejan del concepto cualesquiera *addendas* que puedan entorpecer la calificación del responsable. El elemento subjetivo es "la persona física o jurídica, de naturaleza pública o privada". El elemento objetivo es "el tratamiento", ya que, del ámbito de aplicación ha desaparecido el concepto de fichero y únicamente se define lo que se considera dato personal y tratamiento de datos[130]. No obstante, se protege "todo tratamiento de datos de carácter personal, total o parcialmente automatizado, o realizado de forma estructurada en caso contrario, llevado a cabo, tanto por el sector público, como por el privado"(apdo. 3.1 Propuesta de Madrid).

El elemento funcional es la capacidad de decisión, que se refiere sólo al tratamiento, sin determinar más el objeto ni los aspectos concretos sobre los que versará su capacidad de decisión. Tampoco hallamos en este concepto ningún reenvío a normativa nacional. Lo que se quiere resaltar es la importancia de la decisión sobre el tratamiento, en general. Así se amplía el alcance del concepto, ya que cuando se refiere a aspectos concretos, debe entrarse a valorar si el responsable debe decidir sobre todos ellos o sobre algunos. También debe evaluarse el alcance del poder de decisión respecto a estos aspectos concretos.

[129] *Draft explanatory report of the modernised version of Convention 108, CASHDATA(2014)06, Council of Europe Ad hoc Committee on data protection (CAHDATA), Strasbourg, 23.11.2014*, pág. 5. http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/CAHDATA(2014)06_Draft%20explanatory%20report.pdf (fecha consulta: 28.12.2014).

[130] Finalmente se consigue lo que solicitó hace casi 20 años la autoridad de control francesa (la CNIL) durante el proceso de elaboración de la Directiva 95/46/CE, que pretendía la eliminación del concepto fichero. Ver Capítulo II

En entornos complejos como los tecnológicos, depende de cómo se haga esta valoración puede suponer que queden fuera de la definición muchos de los participantes en los tratamientos. No obstante, no se puede decir que esta sea una opción carente de riesgos. Principalmente, podría llegarse a un concepto demasiado amplio, en el que todo aquel que tenga una mínima capacidad de decisión sobre cualquier aspecto del tratamiento sea considerado responsable. También, podría entenderse que esta capacidad de decisión podría referirse a un momento concreto, lo que también ampliaría demasiado el concepto y correría el riesgo de no asignar bien la responsabilidad.

Finalmente, la madurez del concepto se observa con la inclusión de la corresponsabilidad al indicar "sólo o en compañía de otros". Por otro lado, se incluye en la Propuesta de Madrid un principio denominado "de responsabilidad" (apdo. 11 Propuesta de Madrid) que constituye la introducción en este texto del principio de *accountability* o de rendición de cuentas. Este principio, que como se vió fue desarrollado ampliamente en la Guía OCDE 2013, tiene como objetivo que la persona responsable adopte las medidas necesarias para cumplir con los principios y obligaciones establecidas en el texto. Asimismo, este principio conlleva que el responsable pueda evidenciar este cumplimiento ante los interesados o las autoridades de control[131].

El principio de responsabilidad se conecta con lo que la Propuesta de Madrid denomina "medidas proactivas" (apdo. 22 Propuesta de Madrid). Este catálogo de medidas que los Estados deberían incentivar entre quienes intervengan en el tratamiento, son, por ejemplo, la designación de oficiales de protección de datos, la realización de programas de formación, las auditorías periódicas o la adaptación de los sistemas de información a la legislación, en especial en la etapa de desarrollo. De hecho, la adopción de estas medidas se incentiva ya en el texto, que dispone que podrán ser tenidas en cuenta para fijar la responsabilidad y las sanciones a que deberá hacer frente la persona responsable (apdo. 25 Propuesta de Madrid).

[131] Ver Capítulo IX.

CAPÍTULO II

LA CONSOLIDACIÓN DE LA FIGURA DEL RESPONSABLE EN LA NORMATIVA EUROPEA SOBRE PROTECCIÓN DE DATOS: LA CENTRALIDAD DEL CONCEPTO

Tras la aproximación realizada a los primeros pasos seguidos en la configuración del concepto de responsable, en las primeras leyes nacionales europeas y en los instrumentos internacionales, es en la Directiva 95/46/CE donde esta figura se consolida como parte esencial de la regulación en materia de protección de datos.

Procede examinar, por tanto, los factores que hacen que se considere al responsable como pieza clave de la Directiva 95/46/CE. Una vez se explique la importancia de la figura, se tornará imprescindible determinarla de forma efectiva, ya que, en caso contrario, la construcción de la regulación devendría inservible para su objetivo de protección de los derechos. Por ello, la metodología de análisis del concepto que se presentó en el anterior capítulo se profundiza, con el fin de servir de base para poder determinar al responsable, de acuerdo con los criterios proporcionados, especialmente, por el Grupo del Artículo 29 (GA29) [132].

Con el fin de completar el análisis del concepto en el panorama legislativo europeo, se mencionará su inclusión en otras normas de derecho derivado y se hará una breve mención a la Carta de Derechos Fundamentales de la Unión Europea (Carta UE), referencia obligada al incluir en el catálogo de sus derechos, de forma autónoma, el relativo a la protección de datos.

[132] El Grupo de protección de las personas en lo que respecta al tratamiento de datos personales o Grupo del Artículo 29 (GA29) es un grupo creado en virtud del artículo 29 de la Directiva 95/46/CE y que engloba a las autoridades de control de los Estados miembros de la Unión Europea y de las instituciones y organismos europeos. Es un grupo de carácter consultivo y sus dictámenes, recomendaciones e informes son importantes ya que muestran las opiniones de estas autoridades encargadas de velar por el cumplimiento de las normativas de protección de datos.

1. LA CONSOLIDACIÓN DEL CONCEPTO COMO PIEZA CLAVE EN LA DIRECTIVA 95/46/CE

1.1. El concepto en el proceso de elaboración de la Directiva 95/46/CE

En 1973, la Unión Europea (entonces Comunidad Europea), a través de la Comisión Europea, plasmó la preocupación por la incidencia de la informática, en el ámbito de los derechos y libertades de los ciudadanos, en una Comunicación sobre su propuesta de política comunitaria en materia de tratamiento de datos[133]. Ya en este documento, la Comisión predecía que la estructura de la sociedad se vería determinada en el futuro por la forma en la que se utilizarían los sistemas de información[134].

El año siguiente se iniciaron los primeros debates en el seno del Parlamento Europeo entorno a esta cuestión que concluyeron con la necesidad de elaborar una directiva. Se empezó a trabajar en esta dirección, mientras, paralelamente, emergieron las iniciativas de la OCDE y del Consejo de Europa que resultaron en los textos ya comentados: la Guía OCDE 1980 y el Convenio 108[135]. La aprobación de los mismos, sumado a las dudas que surgieron entorno a la competencia de la Comunidad Europea para intervenir en este ámbito, produjeron la paralización de la elaboración de la Directiva.

La Comisión Europea optó por instar a los Estados miembros para que firmaran y ratificaran el Convenio 108 antes de finalizar 1982, reservándose, si no se cumpliera esta recomendación, el derecho de promover una propuesta legislativa. No obstante, pese a que los Estados miembros no cumplieron con esta recomendación, se retrasó la

[133] *Communication of the Commission of the European Communities to the Council, Community policy on data processing, SEC(73) 4300 final 21.11.1973*, http://aei.pitt.edu/6337/1/6337.pdf (fecha consulta: 10.1.2015), mencionado en *Interim report drawn up on behalf ot the Legal Affairs Committee on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing, reporteur: Lord Mansfield, European Communities, European Parliament, Working documents 1974-1975, Document 487/74, 19.2.1975, PE 39, 608/fin./Annex I*, pág. 11.

[134] *Communication of the Commission of the European Communities to the Council, Community policy on data processing, op.cit.*, pág. 1.

[135] En el informe de *Lord* Mansfield ya se hacía mención a los trabajos llevados a cabo en el seno de la OCDE sobre los riesgos que enfrentaba la privacidad debido a la informatización. *Interim report drawn up on behalf ot the Legal Affairs Committee on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing, reporteur: Lord Mansfield, European Communities, European Parliament, op.cit.*, pág. 11.

elaboración de esta propuesta. Tras la aprobación del Acta Única de 1986[136], la Comisión entendió que la armonización de la normativa en materia de protección de datos era una prioridad para asegurar la libre circulación de datos personales.

Los Estados miembros de la Comunidad Europea mantuvieron sus dudas acerca de la competencia de la Comisión en materia de derechos fundamentales[137]. No obstante, el objetivo primario de la Directiva era la consecución del mercado interior, garantizando la libre circulación de mercancías, personas, servicios y capitales. Para lograr este objetivo era necesaria la libre circulación de datos personales de un Estado miembro a otro y por ello, también era necesario unificar la regulación protectora de estos datos que ya mostraba divergencias (Considerando 3 Directiva 95/46/CE). Basta recordar las diferencias entre las nociones de responsable aparecidas en las primeras leyes europeas o, incluso, la inexistencia de este concepto en algunas de ellas[138].

Con el fin de asegurar que los Estados miembros no pudieran invocar la protección de datos para impedir esa libre circulación de datos, se fijó como objetivo asegurar un alto nivel de protección de este derecho en la Directiva (Considerando 10 Directiva 95/46/CE). Si bien cuando se aprobó la Directiva no se contaba con la plasmación positiva del mismo a nivel europeo, se aludió al derecho al respeto de la vida privada del CEDH, así como a los principios generales del Derecho comunitario, bases jurídicas a las que había acudido la jurisprudencia del Tribunal de Justicia de la Comunidad Europea (actualmente Tribunal de Justicia de la Unión Europea, TJUE) para poder construir una doctrina sobre protección de derechos fundamentales en el marco de la Comunidad Europea[139].

---

[136] Acta Única Europea, 28.2.1986, DO L 169 de 29.6.1987.

[137] De hecho, estas dudas se mantuvieron durante el proceso de elaboración de la Directiva, de forma que algunas delegaciones solicitaron que el Servicio Jurídico de la Comisión se pronunciara sobre la legitimación comunitaria para regular esta materia, que precisó que el objetivo básico de la Directiva no era regular el derecho a la protección de datos sino, en tanto en cuanto, la protección de este derecho podía constituir una restricción de la libre circulación de la información en el seno de la Comunidad. Para reflejar este hecho el Servicio Jurídico propuso el cambio del título de la Directiva para que mostrara este objetivo. *Legal Service opinion, Proposal for a Directive on the protection of individuals in relation to the processing of personal data, 8987/91, European Communities, The Council, Brussels, 30.10.1991,* pág. 4 y Memoria de la Agencia Española de Protección de Datos de 1994.

[138] La Ley francesa de 1978 (*Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*) y las Leyes de Dinamarca de 1978: la Ley 293 que regulaba, por un lado, los ficheros privados (*Danish Private Registers Etc. Act, nº 293, 8 June 1978*) y la Ley 294 que regulaba los ficheros públicos (*Data Public Authorities' Registers Act, nº 294, 8 June 1978*), ambas de 8 de junio de 1978.

[139] Como sí sucede ahora con el artículo 8 Carta UE.

En 1990, la Comisión Europea presentó la primera propuesta de Directiva (Propuesta de Directiva de 1990)[140]. Además de tener en cuenta el Convenio 108, este primer texto se inspiró fundamentalmente en las leyes alemana y francesa vigentes en aquél momento[141].

A raíz de las enmiendas presentadas por el Parlamento Europeo a la Propuesta de Directiva de 1990, la Comisión elaboró una nueva propuesta modificada en 1992 (Propuesta de Directiva de 1992)[142]. Las delegaciones de Alemania, Dinamarca, Irlanda y el Reino Unido presentaron a la Comisión un texto alternativo el 15 de octubre de 1993, que se refería a aquellos puntos sobre los que estos Estados miembros estaban de acuerdo[143]. La importancia de esta contrapropuesta estribaba en la capacidad que estos Estados tenían de constituir en el Consejo una minoría de bloqueo. Finalmente, se acogieron la mayor parte de las propuestas de este grupo y se aprobó la Directiva 95/46/CE[144].

[140] Propuesta de Directiva del Consejo relativa a la protección de las personas en lo referente al tratamiento de datos personales, COM(90) 314 final, DO C 277 de 5.11.1990, pág. 3. Para un estudio pormenorizado del *iter* de esta iniciativa legislativa ver Memoria de la Agencia Española de Protección de Datos de 1994 y M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (Comentario a la Directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos)*, Aranzadi, Cizur Menor (Navarra), 1997, págs. 17 a 45. La propuesta de Directiva la presentó la Comisión mediante la *Commission communication on the protection of individuals in relation to the processing of personal data in the Community and Information security, proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data (SYN 287), COM(90) 314 final-SYN 287 and 288, Brussels, 13.9.1990*, págs. 44 a 70.

[141] El Considerando 11 Directiva 95/46/CE alude expresamente a que "los principios de la protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad, contenidos en la presente Directiva, precisan y amplían los del Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales." Como señala el Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.*, pág. 5, el concepto de responsable del tratamiento se tomó básicamente del Convenio 108 aunque se realizaron algunos cambios que se comentan más adelante. La Memoria de la Agencia Española de Protección de Datos de 1994 alude a la marcada influencia de la Ley federal alemana de protección de datos de 1990, mediante la que se había revisado la Ley anterior de 1977, con el fin de recoger la doctrina sentada por el Tribunal Constitucional Federal en la sentencia relativa a la Ley del censo de 1982 y también se refiere a la influencia de la Ley francesa de 1978.

[142] Propuesta modificada de Directiva del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, COM(92) 422 final, DO C 311 de 27.11.1992, pág. 30.

[143] M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, págs. 41 a 42.

[144] Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO L 281 de 23.11.1995.

Se trata, por tanto, de un largo periplo en el que es interesante internarse para obtener los antecedentes de la regulación final. A continuación se abordará el análisis del concepto de responsable en la directiva y se tendrá en cuenta la evolución del mismo en estos tres textos: la Propuesta de Directiva de 1990, la Propuesta de Directiva de 1992 y el texto final de la Directiva 95/46/CE. Además se integrarán las reflexiones del GA29, plasmadas principalmente en su Dictamen 1/2010[145]. Para realizar el análisis se seguirá el esquema indicado en el anterior capítulo en el que se recorrerán los diferentes elementos que conforman el concepto: subjetivo, objetivo y funcional.

Se reproducen para mayor claridad los conceptos de los textos mencionados:

Propuesta de Directiva de 1990: Artículo 2.e)	**Propuesta de Directiva de 1992:** Artículo 2.d)	**Directiva 95/46/CE:** Artículo 2.d)
"responsable del fichero, la persona natural o jurídica, autoridad pública, servicio o cualquier otro organismo que, con arreglo al Derecho Comunitario o a la legislación de un Estado miembro, sea competente para decidir la finalidad del fichero, qué categorías de datos personales deben registrarse, qué operaciones deben aplicárseles a éstos y a qué terceros está permitido el acceso a los mismos;".	"responsable del tratamiento, la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate u ordene tratar datos personales y decida acerca de la finalidad y los objetivos del tratamiento, los datos personales que deben tratarse, las operaciones que deben aplicárseles y los terceros que pueden tener acceso a dichos datos;"	"responsable del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario;".

[145] Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.*.

1.2. Aspectos del concepto de responsable del tratamiento que lo convierten en elemento esencial de la regulación de la Directiva 95/46/CE

1.2.1. Características del concepto: autónomo, amplio, dinámico y funcional

El concepto de responsable del tratamiento se ha considerado por el GA29 un concepto autónomo del derecho comunitario[146]. Esto significa que el concepto es una disposición de derecho de la UE que no remite expresamente al derecho de los Estados miembros para determinar su sentido y alcance y que será objeto en toda la UE de una interpretación autónoma y uniforme[147]. Para conseguir esta interpretación se tendrá en cuenta, no sólo el tenor de la disposición, sino también el contexto y los objetivos perseguidos por la normativa de la que forme parte, es decir, la Directiva 95/46/CE. El TJUE ha llegado a decir incluso que debe darse a los conceptos autónomos un sentido y alcance idénticos en todos los Estados miembros[148].

No obstante, hay que tener en cuenta que, como se ha visto, el concepto contenido en el artículo 2.d) Directiva 95/46/CE contiene una remisión a la legislación de los Estados miembros y a la comunitaria. Esta remisión, como se comentará más adelante se refiere a la posibilidad de que los fines y los medios del tratamiento estén determinados por esta normativa nacional o comunitaria. En este caso, se brinda la posibilidad de que el responsable del tratamiento o los criterios específicos para su nombramiento se puedan fijar por el derecho nacional. ¿Nos hallamos entonces ante una remisión al derecho de los Estados miembros para determinar el sentido y alcance de este artículo 2.d) Directiva 95/46/CE? ¿Debería entenderse que, en aquellos supuestos en los que los Estados miembros opten por designar al responsable del tratamiento o fijar los criterios para su

[146] Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.*, pág. 9.

[147] Esta jurisprudencia se deriva de la aplicación uniforme del derecho de la Unión y del principio de igualdad. Sentencia del TJUE de 4 de septiembre de 2014 *Vnuk*, C-162/13, EU:C:2014:2146, apdo. 42. En el contexto de la protección de datos, y respecto a un concepto diferente (el de necesidad del artículo 7.e) Directiva 95/46/CE), el TJUE ha considerado que "habida cuenta del objetivo consistente en equiparar el nivel de protección en todos los Estados miembros, el concepto de necesidad, tal como resulta del artículo 7, letra e), de la Directiva 95/46 –cuyo objeto es delimitar con precisión uno de los supuestos en los que resulta lícito el tratamiento de datos personales–, no puede tener un contenido variable en función de los Estados miembros. Por lo tanto, se trata de un concepto autónomo del Derecho comunitario que debe recibir una interpretación idónea para responder plenamente al objeto de dicha Directiva, tal como se define en el artículo 1, apartado 1, de la misma." Sentencia del TJUE de 16 de diciembre de 2008 *Heinz Huber*, C-524/06, EU:C:2008:724, apdo. 52.

[148] Sentencia del TJUE de 16 de junio de 2011 *Omejc* c. *Republika Slovenija*, C-536/09, EU:C:2011:398, apdos. 19 y 21.

nombramiento, deberá respetarse esta regulación nacional aunque pudiera ir en contra de la interpretación que se hubiera dado del artículo 2.d) Directiva 95/46/CE?

Si se respondiera positivamente a estas preguntas, esto implicaría que los Estados miembros podrían apartarse de la interpretación uniforme del concepto de responsable del tratamiento y establecer otras diferentes para designarlo en las leyes que establecieran el nombramiento o los criterios para designar al responsable. También es cierto que, el TJUE no ha proporcionado hasta ahora una interpretación sistemática de los diversos elementos del concepto, por lo que deberíamos esperar a tenerla. Lo que si que hay es la interpretación que han realizado las autoridades de control en el ámbito del GA29 pero que no es vinculante[149].

En todo caso, es coherente con el objetivo de la Directiva 95/46/CE que el concepto de responsable del tratamiento sea un concepto autónomo, ya que ésta persigue la armonización de la regulación en materia de protección de datos y el responsable es una figura clave para esta regulación. Así, es necesario para cumplir con este objetivo de armonización que todos los Estados miembros apliquen el mismo concepto.

Esto implicará que no pueda admitirse que las normas nacionales establezcan conceptos de responsable del tratamiento que vayan en contra del establecido en la Directiva 95/46/CE. Y es que si no se admite una interpretación contraria a la que se realice de un concepto autónomo en el marco del derecho de la Unión, con más razón habrá que rechazar una disposición nacional que vaya en contra directamente del precepto europeo. Las leyes a las que se remite para determinar al responsable tendrán que hacerlo en función de la interpretación del concepto incluido en la ley nacional respectiva, que deberá estar en consonancia con el concepto de la Directiva 95/46/CE.

Como se verá cuando se analice la transposición del concepto en las diferentes normativas nacionales de protección de datos, se han producido importantes divergencias respecto al concepto. No obstante, no se han planteado procedimientos ante el TJUE que hayan suscitado una interpretación por parte del tribunal. La única sentencia importante

[149] El GA29 es un grupo de carácter consultivo (art. 29.1 Directiva 95/46/CE).

que ha abordado el alcance de la definición de responsable, en el asunto *Google*, no ha profundizado en el análisis y los elementos del mismo[150].

El concepto también es autónomo pero, en otro sentido diferente al ya apuntado. Esta autonomía es respecto a la normativa nacional sectorial que se aplique al responsable del tratamiento. Tal como indicaba el GA29, la interpretación del concepto debe realizarse con arreglo a la legislación de protección de datos y no puede verse afectado por otros conceptos de otros ámbitos del derecho que, en ocasiones, podrán solaparse con el de responsable[151].

Una característica que sí que ha dejado clara el TJUE, es que el artículo 2.d) Directiva 95/46/CE contiene una definición amplia, que pretende dar cabida a un amplio espectro de sujetos[152]. De ahí el ámbito extenso, como veremos, de los elementos del concepto.

El GA29 ha señalado que el concepto de responsable del tratamiento es una noción dinámica, en contraposición con la definición de "autoridad controladora del fichero" del Convenio 108, que era una noción estática[153]. De esta forma, el elemento objetivo, como se verá cuando se aborde el mismo, pasa de ser un fichero a un tratamiento de datos. Por tanto, el poder de control del responsable se refiere a una operación o conjunto de operaciones de tratamiento de los datos que reflejan todo el ciclo de vida de los datos, desde que se recogen, hasta que se destruyen[154].

Otro aspecto que puede distorsionar la interpretación del concepto en los diferentes Estados miembros pueden ser las divergencias en la transposición de los

[150] Sentencia del TJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2014:317.
[151] El GA29 menciona como ejemplos el concepto de autor o titular de derechos de propiedad intelectual. Y es que el hecho de ser titular de derechos de propiedad intelectual no excluye la posibilidad de ser también responsable del tratamiento y estar sujeto a las obligaciones en materia de protección de datos. Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.*, pág. 10.
[152] Sentencia del TJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2014:317, apdo. 34.
[153] Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.*, pág. 4.
[154] *Ibídem.*

diversos elementos que conforman la definición, como el concepto de datos personales o el de tratamiento.

El concepto de responsable es funcional, no formal[155]. Esto significa que para determinar si se está ante un responsable debe atenderse, principalmente, a un análisis del supuesto de hecho. En consecuencia, cuando se realice este análisis deberá valorarse si se dan los elementos del concepto. Por tanto, aunque, por ejemplo, a nivel contractual se designe a un sujeto como responsable o pese a que en la notificación a la autoridad de control se haya identificado a un sujeto como responsable, esta calificación podrá decaer ante la realidad[156].

1.2.2. Las funciones del concepto que lo convierten en pieza clave

El TJUE indicó que el objetivo del artículo 2.d) Directiva 95/46/CE, que contiene el concepto de responsable del tratamiento, era, mediante una definición amplia de responsable, garantizar una protección eficaz y completa de los interesados[157]. En consecuencia, las funciones del concepto están orientadas a ese objetivo.

La principal función del concepto de responsable es determinar el sujeto obligado. De esta forma, ante un tratamiento de datos, se proporcionan unos elementos para individualizar al sujeto que los reúna[158]. Este sujeto, será el que deberá cumplir con las

[155] *Ibídem,* pág. 10.

[156] Entre los elementos que GRIMALT SERVERA identificaba en su análisis de la figura del responsable incluía un elemento formal que consistía en la inscripción en el Registro General de Protección de Datos. Entendía este autor que existía una presunción *iuris tantum* de que el sujeto, cuyos datos se habían inscrito en este registro, era el responsable. Si no se había inscrito el fichero, entonces entendía que podía presumirse que quien era el titular de la actividad a la que se vinculaba el tratamiento de datos debía considerarse responsable. P. GRIMALT SERVERA, *La responsabilidad civil en el tratamiento automatizado de datos personales, op. cit.*, págs. 99 a 101.

[157] "[...]el gestor del motor de búsqueda es quien determina los fines y los medios de esta actividad y, así, del tratamiento de datos personales que efectúa él mismo en el marco de ésta y, por consiguiente, debe considerarse «responsable» de dicho tratamiento en virtud del mencionado artículo 2, letra d). Por otro lado, es necesario declarar que sería contrario, no sólo al claro tenor de esta disposición sino también a su objetivo, consistente en garantizar, mediante una definición amplia del concepto de «responsable», una protección eficaz y completa de los interesados, excluir de esta disposición al gestor de un motor de búsqueda debido a que no ejerce control sobre los datos personales publicados en las páginas web de terceros." Sentencia del TJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2014:317, apdos. 33 y 34.

[158] Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.,* pág. 4.

obligaciones que la Directiva 95/46/CE ha establecido para asegurar la protección de los derechos de los interesados.

La determinación del responsable mediante el concepto también permite definir al sujeto que responderá en caso de incumplimiento ante el perjudicado. De esta forma, el responsable tendrá un papel esencial en el sistema de garantías del derecho de protección de datos y en los mecanismos diseñados en la normativa para asegurar esta protección, que pretenden ser preventivos y también reactivos o de reparación[159].

Así, se quiere definir el sujeto al que debe aleccionarse mediante estas medidas para que cumpla con sus obligaciones. De esta forma, las autoridades de control tendrán la posibilidad de supervisar la actividad del responsable para ver si cumple con sus obligaciones. Los interesados tendrán un sujeto ante quien podrán ejercer sus derechos y del que podrán obtener la reparación del perjuicio que puedan haber sufrido por causa del incumplimiento. El responsable, en definitiva, en función de su posición ante el tratamiento, se configura como un garante del derecho a la protección de datos y del cumplimiento de la normativa en esta materia.

Otra función del concepto es delimitar el ámbito de aplicación de la Directiva 95/46/CE y, por tanto, de las legislaciones nacionales que la transpongan. Hay que tener en cuenta que, de acuerdo con una interpretación sistemática de la noción, ésta se halla incardinada en las "Disposiciones generales", que marcan el objetivo de la norma y el ámbito de aplicación. Esto implica que si no se cumpliera con los elementos del concepto no podría activarse el rol de responsable y, por tanto, no se aplicaría la normativa de protección de datos. También hay que tener en cuenta que se deberá cumplir con las otras definiciones con las que se conecta la de responsable, como la de "dato personal" y "tratamiento de datos personales".

En referencia al ámbito de aplicación territorial, el concepto de responsable se utiliza en los criterios que determinan la aplicación de las normativas nacionales de protección de datos (art. 4 Directiva 95/46/CE)[160]. Por último, el concepto de

[159]*Ibídem.* pág. 5. Ver Capítulo VII.
[160]Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.*, pág. 5.

responsable sirve también para determinar el alcance de algunas disposiciones de la Directiva 95/46/CE[161].

1.2.3. La necesidad de una metodología de análisis

Ha quedado clara la importancia del concepto en la regulación de la Directiva 95/46/CE. Al optar por un modelo normativo, en el que la asignación de la responsabilidad se realiza en virtud de la determinación del sujeto obligado, se corre el riesgo, como ha quedado patente, de que no sea clara esta determinación, o bien que pueda ser tan compleja que, en definitiva, se produzca el efecto contrario al deseado: la ausencia de responsabilidad.

Cuando se aprobó la Directiva 95/46/CE los sistemas informáticos estaban más restringidos, ya que el uso de Internet era incipiente y era fácil identificar al responsable. Sin embargo, el uso intensivo de Internet produce una interconexión entre sistemas informáticos. El responsable ya no es un sujeto activo que recoge información directamente del titular de los datos, sujeto pasivo, y lleva a cabo tratamientos sin que los datos salgan de su esfera[162]. Ahora se han creado negocios en los que hay una multitud de sujetos implicados que pueden estar en cualquier parte del mundo y que se conectan unos con otros. La transmisión de datos es automática y se ve favorecida por los propios titulares de los datos que los ofrecen a cambio de atractivos servicios sin coste.

Estos sujetos son los primeros que deben autocalificar su conducta para valorar si pueden encajar en la definición y, en consecuencia, si pueden considerarse responsables del tratamiento. Por lo tanto, las reglas no sólo tienen que estar claras para las autoridades de control que deben aplicar la legislación en caso de vulneración del derecho (y, por lo tanto, para poder dilucidar las responsabilidades necesitan determinar a quién deben

[161] Así, el GA29 cita como ejemplo algunos supuestos del artículo 7 Directiva 95/46/CE, como el del apartado c), cuando establece que el tratamiento podrá efectuarse si es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento o como los artículos 10 y 11 Directiva 95/46/CE cuando incluyen la identidad del responsable del tratamiento como elemento de la información que debe proporcionarse al interesado. *Ibídem*, pág. 8.

[162] O. TENE, "Reforming data protection in Europe and beyond", A. RALLO LOMBARTE, R. GARCÍA MAHAMUT (Ed.), VVAA, *Hacia un nuevo derecho europeo de protección de datos. Towards a new European data protection regime, op. cit.*, pág. 146.

asignarlas), sino que las reglas tienen que estar lo suficientemente claras para que los propios responsables (y, por ende, también los afectados) puedan ubicarse en este rol.

Es necesario contar con un método de análisis que sirva para facilitar esta tarea y, al mismo tiempo, otorgue seguridad jurídica a todos los implicados. Para ello, a continuación, se presentará una metodología que, principalmente, sigue el dictamen del GA29. El GA29 disecciona la definición de responsable en tres partes: la primera, sería el aspecto personal "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo", la segunda, el componente de control plural: "que solo o conjuntamente con otros" y, la tercera, los elementos esenciales que, según el GA29, diferencian al responsable de otros agentes y serán que "determine los fines y los medios del tratamiento de datos personales".

Al igual que se ha visto en el capítulo anterior respecto a los primeros conceptos aparecidos en las leyes nacionales europeas, estimo que es más ilustrativo dividir la definición en elementos: subjetivo, objetivo y funcional. De esta forma, el elemento subjetivo correspondería al aspecto personal señalado por el GA29, el elemento objetivo y el funcional corresponderían a los elementos que diferencian al responsable de otros agentes, según indicaba el GA29[163]. El control plural al que se refiere el GA29 lo he denominado corresponsabilidad. Finalmente, haré referencia al reenvío a otras legislaciones para determinar al responsable, aspecto que, al igual que el GA29, he incluido en el elemento funcional.

Sólo cuando se cumplan los elementos de la definición aplicados a un supuesto determinado, se podrá establecer que el sujeto analizado es responsable del tratamiento.

[163] El GA29 en referencia al componente "determine los fines y los medios del tratamiento de datos personales", inicia el análisis por lo que considera el elemento preliminar que es la palabra "determine" y es aquí donde aborda la cuestión del reenvío a otra legislación para determinar al responsable. Después acomete el análisis del resto del componente, es decir, de "los fines y los medios del tratamiento de datos personales".

2. EL ANÁLISIS DEL CONCEPTO EN LA DIRECTIVA 95/46/CE

2.1. El elemento subjetivo

Antes de abordar el análisis del elemento subjetivo que conforma el contenido de la definición, hay que detenerse en la denominación del responsable. En este sentido, si acudimos a las principales versiones lingüísticas de la Directiva 95/46/CE[164]: en la versión española se le denomina responsable del tratamiento, en la versión en inglés el nombre del sujeto es "*controller*", en la versión en francés es "*responsable du traitement*" y en la versión en italiano es "*responsabile del trattamento"*. Lo que deducimos de estos términos, es que el único divergente es el término inglés. *Controller* se traduce como controlador, por lo que muestra más claramente el rasgo que lo distingue y que es el poder de control sobre el tratamiento[165].

El elemento subjetivo de la figura del responsable se define como "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo". Este elemento refleja exactamente el concepto del Convenio 108 y permanece inalterable prácticamente en los tres textos: la Propuesta de Directiva de 1990, la Propuesta de Directiva de 1992 y la Directiva 95/46/CE[166].

Para facilitar el ejercicio de derechos de los interesados y conseguir una mayor seguridad jurídica con relación a la previsibilidad de quién será considerado responsable, el GA29 indica que debe considerarse responsable del tratamiento preferentemente a la

[164] Hay que tener en cuenta que las versiones auténticas de la Directiva 95/46/CE son todas las versiones en las lenguas oficiales comunitarias, así como la noruega y la islandesa.

[165] Tampoco incluye una alusión al tratamiento, aunque, al especificarse en la definición que se trata de sujetos que determinan los fines y los medios del tratamiento, el hecho de no precisar que el *controller* lo es del tratamiento no parece que tenga ninguna consecuencia relevante.

[166] Lo único que varía es el adjetivo "natural" relativo a "persona" que se sustituye finalmente por "física". En el texto final, hay que mencionar que el Considerando 25 de la Directiva 95/46/CE, que alude a los diversos sujetos que deberán hacerse cargo de las obligaciones establecidas en la Directiva, la lista no coincide exactamente con la que se ha indicado del artículo 2.d), ya que se enumeran los siguientes sujetos: "personas, autoridades públicas, empresas, agencias u otros organismos". Por tanto, se añade el término "agencias", aunque esta referencia hay que entenderla como un error en la coherencia de la traducción, ya que en la versión inglesa se refiere a agencia en los dos supuestos y es en la versión en español donde en el artículo 2.d) se ha traducido como "servicio" y en el Considerando 25 se ha traducido como "agencias". Otra diferencia es la alusión a empresas y a personas en general, sin especificar jurídicas y físicas. En este caso, parece como si se hubiera sustituido la alusión a persona jurídica por la de empresa. Una persona jurídica puede referirse a entidades que no persigan un beneficio, mientras que el término empresa tiene una marcada connotación mercantil.

empresa o al organismo como tal, antes que a una persona concreta que actúe dentro de la empresa o del organismo[167]. De hecho, hay que tener en cuenta que, cuando una persona actúe en el marco de una persona jurídica o de un organismo, pero utilice los datos a los que tiene acceso para sus propios fines, será considerado responsable del tratamiento y, por tanto, activará la responsabilidad del mismo[168].

Con relación al elemento subjetivo, al inicio del proceso legislativo de la Directiva 95/46/CE, se estableció una diferenciación en la regulación del sector público y el sector privado. Esta distinción entre ambos sectores se incluyó en algunas leyes nacionales, como la española.

Si acudimos a las primeras leyes de los países europeos vemos que se realizaron aproximaciones diversas respecto a la regulación de los dos sectores: público y privado. Algunas leyes establecieron una única regulación para ambos sectores, otras leyes incorporaron una doble regulación en el mismo texto legal o se aprobaron leyes diferenciadas para cada uno de los sectores[169].

En el Convenio 108 se regulaba de forma común a ambos sectores. No se siguió este sistema en la Propuesta de Directiva de 1990 que diferenciaba entre la regulación aplicable al sector público y al sector privado en materia de legitimidad del tratamiento de los datos y derecho de acceso[170]. De esta forma, se realizaba una aproximación diferente en la regulación, dependiendo del tipo de responsable.

---

[167] Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.*, pág. 17.

[168] *Ibídem.*

[169] Ejemplos de ley que se aplicaba indistintamente a los dos sectores era la Ley francesa de 1978 (*Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*) y la Ley sueca de 1973 (*Datalag* 1973:289). Como ejemplo de regulación dual, además de la Ley federal alemana de 27 de enero de 1977 (*Bundesdatenschutzgesetz*, BDGS), la Ley luxemburguesa de 1979 (*Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques)* que con relación a la creación y explotación de los ficheros distinguía entre los que trataba el Estado y los que trataban el resto de responsables. Como ejemplo de leyes independientes para los dos sectores, estaban las leyes danesas: Ley nº 293 reguladora de los ficheros del sector privado (*Danish Private Registers Etc. Act, nº 293, 8 June 1978*) y Ley nº 294 reguladora de los ficheros del sector público (*Data Public Authorities' Registers Act, nº 294, 8 June 1978*), ambas de 8 de junio de 1978.

[170] Se incluían en su artículo 2, apartados g y h, definiciones de lo que se consideraba sector público ("el conjunto de las administraciones, organismos y entidades de un Estado miembro sujetos al Derecho público (con excepción de aquellas que participen en una actividad industrial o comercial) y los organismos y entidades de Derecho privado que participen en el ejercicio de la autoridad pública"), y sector privado ("toda persona natural o jurídica, o asociación (administraciones, organizaciones y entidades del sector público inclusive) en la medida en que ejerza una actividad industrial o comercial").

Esta duplicidad provenía de la influencia de la Ley federal alemana de 1990 que diferenciaba las condiciones de licitud para el tratamiento de datos según lo realizara el sector público o el sector privado. Esta ley partía de la prohibición de todo tratamiento de datos sin contar con el consentimiento del interesado o sin que existiera una ley que lo habilitara[171]. De esta forma, en la Propuesta de Directiva de 1990, se establecía para el sector privado la regla general de solicitud de consentimiento para poder tratar datos y para el sector público la legitimación si el tratamiento era preciso para que el responsable pudiera llevar a cabo sus cometidos como autoridad pública.

En la Propuesta de Directiva de 1992 desapareció esta distinción entre sector público y privado debido a que algunos Estados habían alegado que les planteaba dificultades adaptarse a este sistema[172]. En consecuencia, se estableció una regulación común para la legitimación de los tratamientos que incluyó como un presupuesto más de legitimación el consentimiento de los afectados.

No obstante, sí se especificó en la parte de considerandos que sería la legislación de los Estados miembros la que determinaría si el responsable del tratamiento que tuviera conferida una misión de interés público debería ser una administración pública u otra persona de derecho público o privado (Considerando 32 Directiva 95/46/CE)[173]. Esta previsión se refiere a una de las bases jurídicas que legitimarán al responsable para poder llevar a cabo un tratamiento: cuando el mismo sea necesario para el cumplimiento de una

[171] M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, págs. 30 a 33. Hay que tener en cuenta que la Ley federal alemana de 1990 que revisó la de 1977 se aprobó el 20 de diciembre de 1990, tras la aprobación de la Propuesta de Directiva de 1990, el 25 de julio de 1990, por lo que la elaboración de ambas transcurrió de forma paralela. Entiendo que el autor, al mencionar la Ley federal alemana de 1990, como inspiración de la Propuesta de Directiva de 1990, se refiere a los trabajos preparatorios de la misma.

[172] Así lo manifestó especialmente la delegación irlandesa, a la que se unieron las delegaciones del Reino Unido, la francesa, griega y belga. El resto de delegaciones no vieron problema en dejar la elección en manos de los Estados miembros. *Outcome of proceedings of Working Party on Economic Questions (Data Protection) on 19 and 20 June 1991, 7284/91, European Communities, The Council, Brussels, 19.7.1991,* págs. 7 a 9.

[173] Considerando 32 de la Directiva 95/46/CE: "Considerando que corresponde a las legislaciones nacionales determinar si el responsable del tratamiento que tiene conferida una misión de interés público o inherente al ejercicio del poder público, debe ser una administración pública u otra persona de derecho público o privado, como por ejemplo una asociación profesional;". No obstante, ya se establece en su considerando 35 que se entenderá que las asociaciones religiosas reconocidas oficialmente sí realizan tratamientos de datos personales por motivos importantes de interés público.

misión de interés público o inherente al ejercicio del poder público conferido al responsable o a un tercero a quien se comuniquen los datos (art. 7.e) Directiva 95/46/CE).

No debe confundirse la determinación del responsable del tratamiento con el fundamento de la legitimación para tratar datos. En el sector público existe una tendencia a conectar estos dos aspectos, de forma que se identifica al responsable en función de las competencias que otorgan la legitimación para poder tratar datos. Si bien es cierto que lo habitual es que las cuestiones vayan unidas, no siempre será así.

2.2. El elemento objetivo

Para entender el elemento objetivo sobre el que el responsable actuará es necesario analizar, primero, los diferentes conceptos que integran este objeto material. Y es que la figura del responsable se incardina en la parte que la Directiva 95/46/CE dedica a determinar su ámbito de aplicación. El artículo 2 Directiva 95/46/CE se refiere a dos grupos de definiciones, el relativo al ámbito objetivo y el relativo al ámbito subjetivo. El ámbito objetivo se compone de "datos personales", "tratamiento de datos personales" y "fichero de datos personales". El ámbito subjetivo integraría las definiciones de "responsable del tratamiento", "encargado del tratamiento", "destinatario" y la de "interesado", ésta última incluida en la definición de datos personales.

Todas estas definiciones se interrelacionan para componer el ámbito al que se aplicará la Directiva 95/46/CE. Se abordan a continuación las definiciones relativas al objeto sobre el que actúa el responsable. Hay que precisar que en el análisis del ámbito de aplicación de la Directiva 95/46/CE faltaría hacer referencia al ámbito territorial. No obstante, esta cuestión se analizará posteriormente[174].

2.2.1. Datos de carácter personal

Como indica el GA29, definir el concepto de "datos personales" equivale a definir lo que entra o queda fuera del ámbito de aplicación de las normas sobre protección de

[174] Ver Capítulo IV.

datos[175]. Y esto equivale también a decir lo que el responsable del tratamiento deberá proteger o no, al cumplir con esas normas.

La definición de dato personal de la Directiva 95/46/CE no detalla qué tipo de información se considerará dato personal. Sin embargo, esta definición refleja la intención del legislador de adoptar una noción amplia en la que incluir toda la información que pueda vincularse a una persona[176]: "datos personales: toda la información sobre una persona física identificada o identificable (el interesado)" (art. 2.a) Directiva 95/46/CE).

Para saber cuando nos hallaremos ante una persona física, habrá que acudir a los ordenamientos jurídicos de los Estados miembros donde se establecerá la definición de personalidad. En principio no serán objeto de protección los datos que puedan tratarse de fallecidos y de personas jurídicas[177]. No obstante, nada impide a los Estados miembros que extiendan el alcance de protección de la normativa de protección de datos a estos colectivos[178]. Asimismo, esta mención a la persona refleja que el derecho de protección de datos es un derecho que protege a los seres humanos y un derecho universal que no permite discriminar entre nacionales y extranjeros[179].

[175] Dictamen 4/2007 sobre el concepto de datos personales, 012480/07/ES WP 136, 20.6.2007, Grupo de trabajo Artículo 29 sobre la protección de datos, pág. 3.

[176] *Commission communication on the protection of individuals in relation to the processing of personal data in the Community and Information security, proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, op. cit.*, pág. 19.

[177] El Considerando 24 Directiva 95/46/CE establece que "las legislaciones relativas a la protección de las personas jurídicas respecto del tratamiento de los datos que las conciernan no son objeto de la presente Directiva". No obstante, como indica el GA29 en su Dictamen 4/2007, *op. cit.*, p.24-26, cabe realizar alguna matización, ya que estos datos pueden recibir cierta protección si, por ejemplo, el responsable, en el caso de una persona fallecida, ignora que ésta ha fallecido y sigue protegiendo sus datos, creyendo que son aún datos personales, o si, en el caso de personas jurídicas adopta la medida de proteger indistintamente los datos de personas físicas y jurídicas, ante la dificultad de separar los datos de ambos colectivos.

[178] De hecho Italia, Austria o Luxemburgo han extendido la protección a las personas jurídicas. De la misma forma, los Estados miembros pueden extender el alcance de su normativa nacional de protección de datos cuando no resulte aplicable la Directiva 95/46/CE, por no considerarse datos de carácter personal según los criterios indicados, siempre que ninguna norma de Derecho comunitario se oponga a ello. Dictamen 4/2007 sobre el concepto de datos personales, *op. cit.*, pág. 26-27 y Sentencia del TJUE de 6 de noviembre de 2003 *Bodil Lindqvist*, C-101/01, EU:C:2003:596, apdo. 98.

[179] El Considerando 2 de la Directiva 95/46/CE establece que "los sistemas de protección de datos están al servicio del hombre; que deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y derechos fundamentales de las personas físicas y, en particular, la intimidad, y contribuir al progreso económico y social, al desarrollo de los intercambios, así como al bienestar de los individuos;"

Un dato para que sea objeto de protección de la Directiva debe poder vincularse con una persona identificada o identificable, lo que la cualificaría como dato de carácter personal[180]. Una cuestión nada simple será el hecho de valorar cuando una persona debe considerarse identificable. La definición ofrece la siguiente pauta "se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

Según esta definición una persona será identificable si su identidad puede determinarse directa o indirectamente. Para ilustrar cómo se puede lograr esta identidad, la definición menciona la utilización de lo que el GA29 ha denominado como "identificadores"[181]. Se trata de datos concretos que tienen una relación privilegiada y muy cercana con una determinada persona. Ejemplo de ello sería la apariencia exterior de la persona (la altura, el color de pelo) o cualidades que no se ven externamente, como su profesión, su nombre, un número de teléfono, el número de documento nacional de identidad o el de pasaporte, el de la seguridad social, la matrícula del coche, la IP del ordenador o el código interno asignado en una base de datos.

Lo normal será que una persona se identifique directamente mediante su nombre y apellidos. Asimismo, aunque no se tengan su nombre y apellidos, se podrá identificar a esta persona de forma indirecta si se acumulan otros datos que la lleguen a singularizar[182]. En este sentido, serán esenciales las circunstancias concretas de cada caso, de forma que, pese a que se tengan su nombre y apellidos, puede que tampoco esto permita identificar a una persona, si se realiza en el marco de la población de un país, donde puede haber más de una que se llame igual[183].

Hay que mencionar la sentencia del TJUE en el asunto *YS*, ya que entiendo que iría en contra de esta noción amplia de dato personal[184]. Esta sentencia responde a una cuestión prejudicial en la que se suscita si la información contenida en un documento interno, que forma parte de un expediente administrativo de tramitación de una solicitud

[180] M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, pág. 73.
[181] Dictamen 4/2007, sobre el concepto de datos personales, *op. cit.*, pág. 13 a 14.
[182] *Ibídem*, pág. 15
[183] *Ibídem*, pág. 14.
[184] Sentencia del TJUE de 17 de julio de 2014 *YS*, C-141/12 y C/372/12, EU:C:2014:2081.

de residencia, se puede considerar que contiene datos personales del solicitante. Esta cuestión se enmarca en varios supuestos de ejercicio del derecho de acceso, por parte de solicitantes, a los que se había denegado la entrega del mencionado documento[185].

Pues bien, el TJUE distingue dos tipos de información en este documento: la que se refiere a los datos del solicitante y de los agentes que intervienen en la redacción y supervisión del documento y la que contiene el análisis jurídico que realizan los agentes en virtud de los datos del solicitante aportados. En la sentencia, el TJUE entiende que los datos del solicitante deben calificarse de datos personales, de acuerdo con la Directiva 95/46/CE pero no el análisis jurídico[186]. Hay que matizar que el tribunal admite que el análisis jurídico puede incorporar datos personales pero que la valoración jurídica no puede estimarse dato personal en sí misma[187].

El tribunal justifica esta diferenciación en virtud del alcance que debe darse al ejercicio del derecho de acceso, en conexión con el objetivo de la Directiva 95/46/CE. Así, el TJUE afirma que extender el derecho de acceso a este análisis jurídico no sirve al objetivo de garantizar el derecho a la intimidad del solicitante, sino que serviría para garantizarle el derecho de acceso a los documentos administrativos[188]. Por tanto, este planteamiento del tribunal tiene en cuenta que la protección frente a la valoración jurídica realizada vendría de la mano de otro derecho.

Para determinar si una persona es identificable hallamos un criterio en la parte de los considerandos: "los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona" (Considerando 26 Directiva 95/46/CE). No siempre que se pueda llegar a identificar a una persona deberá considerarse que ésta es identificable, ya que deberán tenerse en cuenta otros factores, como el coste de llegar a esa identificación, el posible desarrollo tecnológico en el momento del tratamiento y posteriormente, mientras se traten los datos,

[185] El Ministro de Inmigración, Integración y Asilo de los Países Bajos, competente para responder las solicitudes de permisos de residencia, entregó hasta 14 de junio de 2009 estos documentos internos cada vez que se solicitaba pero, finalmente dejó de hacerlo, ya que originaban una gran carga de trabajo y, a menudo, los solicitantes malinterpretaban los análisis jurídicos incluidos. Asimismo, se detectó que estos documentos recogían cada vez menos el intercambio de pareceres en el servicio. *Ibídem*, apdo.16.
[186] *Ibídem*, apdo. 48.
[187] *Ibídem*, apdos. 39, 48.
[188] Hay que recalcar que se menciona el derecho a la intimidad y no el derecho a la protección de datos en la sentencia. *Ibídem*, apdo. 46.

la finalidad perseguida por el responsable con el tratamiento o incluso el riesgo de que se produzca un incidente que afecte a la seguridad del tratamiento[189].

Respecto al factor de la finalidad del tratamiento, el GA29 ha indicado que, cuando un responsable lo que persigue con el tratamiento es identificar, en algún momento, al interesado, resultaría una contradicción flagrante, alegar que no se tratan datos personales[190]. Un ejemplo sería el tratamiento de datos con fines de videovigilancia, en el que la finalidad última será identificar al afectado[191].

El GA29 resalta la utilización de medidas de seguridad, técnicas y organizativas, para evitar que se pueda identificar a las personas, de forma que evite la aplicación de la normativa[192]. Se diferencia entre el proceso de hacer anónimos los datos y otras medidas, como el uso de seudónimos o el cifrado.

Si los datos son anónimos, de forma que se evite la identificación del interesado, no se aplicarán los principios de protección de datos (Considerando 26 Directiva 95/46/CE). En caso de optar por esta opción, el GA29 tiene en cuenta el criterio de la razonabilidad de los medios para evaluar si el proceso de anonimizar los datos es suficientemente consistente para hacer imposible la identificación[193].

---

[189] El GA29, en lo que se refiere al factor del desarrollo tecnológico, entiende que se trata de una prueba dinámica. Si los datos se conservan durante un breve período de tiempo, puede que no sea factible alcanzar la identificación de la persona durante el ciclo de vida del tratamiento. Pero si el período de conservación es largo podría llegar a alcanzarse la identificación debido a la rapidez en la que avanzan los medios tecnológicos existentes y, por lo tanto, esos datos deberían considerarse datos personales. En cuanto al criterio de la finalidad del tratamiento, el hecho de que un responsable del tratamiento trate datos de una persona que no está identificada, con la finalidad de llegar a identificarla (p.ej. cuando se tratan datos con la finalidad de videovigilancia) supone para el GA29 asumir que ese responsable tiene o puede tener medios que puedan ser razonablemente utilizados para identificar a esa persona. Dictamen 4/2007, sobre el concepto de datos personales, *op. cit.*, pág. 17.

[190] *Ibídem.*

[191] *Ibídem*, pág. 16 y 18. En el caso de la videovigilancia, lo cierto es que los medios que deberá tener en cuenta el responsable serán los que tengan las autoridades que investigarán en caso de que se produzca un incidente. En consonancia con el mencionado Considerando 26 Directiva 95/46/CE el responsable deberá tener en cuenta, no sólo sus propios medios sino los de estos terceros que pueden intervenir. Del mismo modo, se alude al riesgo de un incidente de seguridad, en el que también habrá que valorar los medios de que dispondrá el tercero atacante, que puede hacerse con los datos, para identificar a los interesados. Lo que se persigue es un alto grado de protección.

[192] *Ibídem*, pág. 19.

[193] En este sentido, el GA29 advierte que no se pueden fijar las circunstancias que harán que no sea posible esta identifcación, debido a la evolución continua de la tecnología. Sin embargo señala algunos factores, como el examen que debería realizar el responsable de los medios que precisaría para revertir la técnica utilizada para anonimizar, especialmente en términos de costes y conocimientos asociados al uso de estos medios. También indica que cuando el responsable no borre los datos originales, aunque entregue parte de los mismos y elimine los datos identificables, estos datos resultantes seguirán siendo datos personales.

De nuevo, el responsable, no sólo debe limitarse a los medios que tenga a su disposición, sino a los que pueda tener otra persona. De esta forma, el GA29 ha interpretado que, incluso en el caso de que el responsable del tratamiento proporcione a un tercero un conjunto de datos sometido a una técnica de anonimización, el tercero deberá tener en cuenta los mismos factores que el responsable, cuando lleve a cabo el proceso[194]. Si existieran riesgos de identificación de los interesados, se volvería a aplicar la normativa y esto le podría acarrear a este tercero que se le considerara responsable.

El proceso de valoración que sigue el GA29 para considerar si los datos son anónimos es muy estricto y, de nuevo, hay que estar al caso concreto. La conclusión que se desprende es que, sólo si no es posible la reversión del proceso se estará ante datos anónimos.

Otros procesos diferentes son utilizar seudónimos o el cifrado de datos[195]. Si bien, se considera que el uso de estos procesos conlleva un menor riesgo para los datos de los individuos afectados, no son equiparables a la técnica para anonimizar, ya que permiten volver a vincular los datos a las personas, cuando lo decida el responsable. Este mecanismo constituye, más bien, una medida de seguridad, ya que dificulta la vinculación de un conjunto de datos con la identidad de un titular de datos[196].

2.2.2. Fichero

En la Propuesta de Directiva de 1990 se definió al responsable como "responsable del fichero". Esta denominación fue consecuencia de centrar el objeto de la regulación en el fichero o archivo automatizado, al igual que se había hecho en el Convenio 108 del Consejo de Europa. Además también se incluyó, como en el Convenio 108, una definición de tratamiento que lo que hacía era completar la de fichero. No obstante, a diferencia del Convenio 108, en la Directiva se amplió el alcance del concepto de fichero, no sólo a los automatizados, sino también a ficheros "manuales" (como pueden ser

---

Dictamen 5/2014 sobre técnicas de anonimización, 0829/14/ES WP 216, 10.4.2014, Grupo de trabajo Artículo 29 sobre la protección de datos, pág. 9 a 11.

[194] *Ibídem*, pág. 11.

[195] Dictamen 4/2007, sobre el concepto de datos personales, *op. cit.*, págs. 19 a 24.

[196] Dictamen 5/2014 sobre técnicas de anonimización, *op. cit.*, pág. 3.

aquellos en los que los datos figuran en soporte papel) y se detalló más la definición de fichero[197].

Durante el proceso de elaboración de la Directiva 95/46/CE, la autoridad de control francesa (la *Commission Nationale de l'Informatique et des Libertés* o CNIL), enseguida manifestó su reticencia a admitir el papel preponderante de este concepto de fichero, ya que consideraba que había quedado desfasado y no incluía estructuras, como las bases de datos[198]. Por eso, esta autoridad propuso su sustitución y, de ese modo, dejar sólo el término "tratamiento" que era más general[199].

Pese a las sugerencias de la autoridad de control francesa de eliminar la noción de fichero, la Comisión Europea decidió no suprimirlo[200]. La Comisión reconoció que el concepto debía considerarse obsoleto pero juzgó necesario mantenerlo, con objeto de preservar dentro del ámbito de aplicación de la Directiva los ficheros manuales. No obstante, el concepto de fichero se utilizó para limitar los tratamientos no automatizados que entrarían en el ámbito de aplicación, de forma que sólo se incluirían aquellos datos que formaran parte de un fichero o fueran a ser parte del mismo[201]. Por tanto, el concepto de fichero se refiere a los datos procesados de forma no automatizada[202].

En el texto definitivo de la Directiva 95/46/CE, su ámbito de aplicación se extiende a los tratamientos total o parcialmente automatizados, así como a los tratamientos no automatizados de datos personales contenidos o destinados a ser incluídos en un fichero (art. 3.1 Directiva 95/46/CE). Esto se completa con la definición de «fichero de datos personales» o «fichero» como "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica" (art. 2.c) Directiva 95/46/CE). Si quedaba

[197] La definición del Convenio 108 de "fichero automatizado" era "cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado" (art. 2.b Convenio 108). La definición de la Propuesta de Directiva de 1990 era: "todo conjunto de datos personales, centralizados o repartidos en diversos emplazamientos, que sean objeto de un tratamiento automatizado o que, sin serlo, estén estructurados y sean accesibles dentro de una recopilación organizada según criterios determinados con objeto de facilitar su utilización o interconexión;" (art. 2.c Propuesta de Directiva de 1990).
[198] M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, pág. 77.
[199] *Ibídem*, pág. 78. Y es que la Ley francesa de 1978 se centraba en la noción de tratamiento.
[200] *Ibídem*.
[201] *Ibídem*.
[202] *Ibídem*, pág. 79.

alguna duda, en la parte de considerandos, se aclara que, cuando se trate de tratamientos manuales, sólo se aplicará la Directiva 95/46/CE a los ficheros (Considerando 27 Directiva 95/46/CE).

Durante la elaboración de la Directiva también surgió la duda sobre qué cabía interpretar exactamente como ficheros manuales[203]. Finalmente, se especifica que no se aplicará la Directiva 95/46/CE a las carpetas no estructuradas y que los criterios para determinar los elementos del conjunto estructurado de datos que conforma el fichero y los criterios que regulan el acceso a este conjunto de datos se dejan en manos de los Estados miembros (Considerando 27 Directiva 95/46/CE).

2.2.3. Tratamiento

El tratamiento, como ya se ha mencionado anteriormente, se concibe como elemento clave para determinar el ámbito de aplicación material de la directiva y releva al término "fichero", eje de la primera Propuesta de Directiva de 1990. La definición de tratamiento también es amplia, al implicar:

> "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción" (art. 2.b) Directiva 95/46/CE).

Por lo tanto, se trata de un abanico extenso de operaciones que pretende cubrir cualquier manejo de los datos. Como ejemplo se puede citar la sentencia del TJUE, asunto *Lindqvist* en la que el tribunal consideró que "hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número

[203] Pese a que en la versión española de la Directiva 95/46/CE se habla de "carpeta" la discusión en el procedimiento de elaboración de la misma se centró en el concepto de expediente (*folder, dossier, Akte*). El expediente se hallaba definido en la Ley federal alemana: "es expediente todo otro documento destinado a cualesquiera otros fines oficiales o de servicio, incluso los que consistieren en soportes de imágenes o de sonido. No son expedientes los anteproyectos y notas que no formaren parte del asunto" que además dejaba claro que no se consideraba fichero: "no son ficheros los expedientes y colecciones de expedientes, a menos que puedan ser reordenados y explotados por procedimientos automáticos". *Memoria de 1994*, de la Agencia de Protección de Datos, M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, pág. 79, y P. GRIMALT SERVERA, *La responsabilidad civil en el tratamiento automatizado de datos personales, op. cit.*, pág. 69.

de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un tratamiento total o parcialmente automatizado de datos personales"[204].

En la propuesta inicial se extrajo de esta lista la recogida de datos debido al hecho de que como ya se ha indicado se inspiraba en la Ley federal alemana de 1990 y, en esa norma, la recogida de datos, tenía una regulación específica[205]. No obstante, en el trámite de elaboración de la Directiva se optó por incluir la recogida en la definición de tratamiento, ya que se consideró una fase más del mismo[206].

Evidentemente, esta definición es más amplia que la que se especificó en el Convenio 108, ya que en éste se refería sólo a ficheros automatizados y, por tanto, se orientaba a cubrir sólo operaciones que pudieran realizarse de forma electrónica. Además en la Directiva se añaden operaciones tan importantes como la consulta o la conservación.

2.2.4. Exclusiones del ámbito de aplicación

Por último, para tener una visión completa del objeto sobre el que va a poder actuar el responsable, además de los elementos que hemos incluido en el mismo, también hay que tener en cuenta las exclusiones que establece la Directiva en su ámbito de aplicación (art. 3.2 Directiva 95/46/CE).

La primera exclusión se relaciona con el ámbito de aplicación del Derecho comunitario. Esta exclusión originó debates entorno a cómo detallar las materias a las que no se aplicaba este derecho[207]. Finalmente, se estableció que la Directiva 95/46/CE no se aplicaría al tratamiento de datos personales, efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del derecho comunitario. Se enumeraban, a modo de ejemplo, las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y las que se refirieran a la seguridad pública, la defensa, la seguridad

[204] Sentencia del TJUE de 6 de noviembre de 2003 *Bodil Lindqvist*, C-101/01, EU:C:2003:596, apdo. 27.
[205] M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, pág. 75.
[206] El Dictamen del Comité Económico y Social propuso que se incluyera la recogida en la definición de tratamiento. *Ibídem*, pág. 75.
[207] M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, págs. 87 a 89.

del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal[208].

Como ejemplo de un supuesto en el que el TJUE ha entendido que se debían aplicar estas exclusiones, se puede citar el asunto del Acuerdo sobre el PNR (*Passenger Name Record*) con EEUU[209]. Este acuerdo entre la UE y los EEUU, celebrado a raíz de los atentados terroristas del 11S, permitía el traspaso por parte de las compañías aéreas de sus viajeros europeos al Servicio de aduanas de EEUU, con la finalidad de luchar contra el terrorismo y la delincuencia grave. El TJUE anuló la Decisión 2004/535/CE de la Comisión, mediante la que declaraba el carácter adecuado de protección, en el marco de este acuerdo, por entender que esta materia quedaba fuera del ámbito de aplicación de la Directiva 95/46/CE, según su artículo 3.2[210]. Asimismo, el tribunal también anuló el acuerdo con los EEUU, por la misma razón, al haberse adoptado en virtud de una base jurídica referida al mercado interior[211].

Pese a que las actividades, desglosadas en este precepto 3.2 Directiva 95/46/CE, se enuncian como una lista no exhaustiva de supuestos excluidos, se ha estimado que debe realizarse una interpretación estricta. En este sentido, se ha entendido que esta enumeración, en realidad, delimita el alcance de la excepción, que sólo se aplicará a las que se mencionan expresamente o que pueden incluirse en la misma categoría[212].

La segunda exclusión se refiere a todo tratamiento efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas. En la parte

[208] Hay que recordar que el Tratado de Maastricht de 1992 introdujo la estructura de pilares que dividían las competencias de la UE y que fue eliminada con el Tratado de Lisboa de 2007. El primer pilar era el pilar comunitario, donde se incluían las cuestiones supranacionales y que correspondía a las tres comunidades (Comunidad Europea, Comunidad Europea de la Energía Atómica o Euratom y Comunidad Europea del Carbón y del Acero o CECA). El segundo pilar era el correspondiente a la política exterior y de seguridad común regulada en el título V del TUE. El tercer pilar era el correspondiente a la cooperación policial y judicial en materia penal, regulado en el título VI del TUE. Ante la eliminación de la estructura en pilares, hay que esperar a la aprobación de nueva normativa que se adapte al nuevo modelo. Ver Capítulo IX.

[209] Sentencia del TJUE de 30 de mayo de 2006, *Parlamento Europeo/Consejo de la Unión* Europea y Comisión C-317/04 y C-318/04, EU:C:2006:346.

[210] Decisión 2004/535/CE de la Comisión, de 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos.

[211] Decisión 2004/496/CE del Consejo, de 17 de mayo de 2004, relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos.

[212] Sentencia del TJUE de 6 de noviembre de 2003 *Bodil Lindqvist*, C-101/01, EU:C:2003:596, apdo. 44.

de considerandos e cita como ejemplo de este tipo de actividades: la correspondencia y la llevanza de un repertorio de direcciones (Considerando 12 Directiva 95/46/CE). Si bien en las Propuestas de Directiva de 1990 y de 1992 se indicaba "actividades privadas y personales" al final se sustituyó "privadas" por "domésticas", término sin duda más elocuente.

Es obligado señalar que la importante sentencia *Lindqvist* matizó esta disposición, de forma que la difusión por Internet de datos que realice una persona física a un grupo indeterminado de personas no se entiende dentro de esta exclusión[213].

El TJUE, en el asunto *Rynes*, tampoco entendió excluido el tratamiento de datos realizado mediante la utilización de un sistema de videovigilancia por cámaras, con la finalidad de proteger un domicilio de un particular[214]. Hay que tener en cuenta, que en el caso planteado, la videocámara abarcaba espacio público, aspecto que tuvo en cuenta el TJUE para indicar que se había desbordado la esfera privada del particular considerado responsable del tratamiento. Por ello, no se podía considerar que la actividad fuera "exclusivamente personal o doméstica", a efectos del artículo 3.2 Directiva 95/46/CE[215]. En este asunto, el TJUE recalcó también el carácter estricto de la interpretación que cabía realizar del supuesto de exclusión[216].

2.3. El elemento funcional

En este apartado relativo al elemento funcional se analizará la acción concreta que efectúa el responsable sobre el elemento objetivo descrito anteriormente, acción que se describe con la palabra "determine". La identificación del responsable se efectuará así mediante el análisis de si el sujeto que actúa sobre el objeto tiene esta capacidad de determinación, que además se focalizará en unos aspectos concretos. Estos aspectos concretos son: "los fines y los medios del tratamiento".

Si estos fines y medios se determinan por disposiciones legislativas o reglamentarias nacionales o comunitarias, la fijación de quién será responsable del

[213] *Ibídem*, apdo. 47.
[214] Sentencia del TJUE de 11 de diciembre de 2014 *Rynes*, C-212/13, EU:C:2014:2428.
[215] *Ibídem*, apdo. 33.
[216] *Ibídem*, apdos. 30 y 31.

tratamiento o los criterios específicos para identificarlo podrán establecerse en esta legislación. Aparece, por tanto, un reenvío a otras normas para llevar a cabo esta determinación del responsable. Este reenvío dará pie al análisis de las fuentes de las que emana el control que ostenta el responsable y que servirán para determinarlo. Existe la posibilidad de que se identifiquen no uno, sino una pluralidad de responsables, cuestión que también se abordará. Por último, se hará referencia al tratador efectivo para poner el acento en la identificación del responsable, no en la realización material del tratamiento, sino en el poder de decisión que ostente el sujeto.

2.3.1. Aspectos concretos sobre los que recae la capacidad de determinación del responsable: los fines y los medios del tratamiento de datos personales

En la Propuesta de Directiva de 1990, el responsable era competente para decidir sobre: la finalidad del fichero, las categorías de datos personales que deben registrarse, las operaciones que deben aplicárseles a estos datos y a qué terceros está permitido el acceso a los mismos. En la Propuesta de Directiva de 1992 el responsable decidía acerca de: la finalidad y los objetivos, esta vez, del tratamiento; los datos personales que deben tratarse, las operaciones que deben aplicárseles y los terceros que pueden tener acceso a dichos datos.

En la versión definitiva de la Directiva 95/46/CE el responsable determina los fines y los medios del tratamiento de datos personales. Por lo tanto, a primera vista parece que se reduce la capacidad de decisión del responsable mediante una simplificación progresiva de estos aspectos en los diversos textos del proceso legislativo. Se mantiene la finalidad en todos ellos pero, en vez de datos personales, operaciones y terceros, se utiliza el término medios que bien podría englobar las operaciones a las que se someterán los datos, pero difícilmente puede entenderse que incluye los datos personales y los terceros.

De la interpretación literal de esta simplificación se deduciría que no se considera esencial para determinar quién es el responsable su capacidad de decisión respecto a los elementos suprimidos. Así, por ejemplo, si el responsable no decidiera sobre los datos personales que se recogen, de todas formas podría considerarse responsable. Sin embargo,

el GA29 no comparte este primer análisis. Sin duda, como también afirma el GA29, los fines y medios parecen responder a las preguntas "por qué" y "cómo" del tratamiento[217].

El GA29 interpreta que con relación a los medios debe considerarse que la reducción que se lleva a cabo en el proceso legislativo no implica la sustracción de elementos, sino que se trata de una fórmula abreviada[218]. Los medios se referirán, por tanto, no sólo a los medios técnicos utilizados para realizar el tratamiento, sino también al "cómo" que incluirá la determinación de los datos, las operaciones a realizar y los terceros que tendrán acceso a los datos.

No obstante, el GA29 diferencia dos categorías de elementos a los que se referiría el término "medios": los medios técnicos y organizativos (p.ej. ¿qué software o hardware debe utilizarse?) y los elementos esenciales, que son aquellos que se reservarían para ser determinados por el responsable del tratamiento (p.ej. ¿qué datos deben tratarse?, ¿durante cuánto tiempo?, ¿quién debe tener acceso a ellos?)[219].

La determinación de los fines nos llevará siempre a la identificación del responsable, ya que es claramente un aspecto primordial del tratamiento. Con relación a los medios, será posible que los medios técnicos y organizativos los pueda determinar el encargado del tratamiento. Sin embargo, la determinación de los elementos considerados esenciales corresponderá al responsable del tratamiento.

En esta línea, el GA29 indica que en algunos sistemas jurídicos las decisiones adoptadas respecto a las medidas de seguridad, adoptadas para proteger los datos, son especialmente importantes y deberán considerarse un medio esencial[220]. Al final debe tenerse en cuenta lo que establece la legislación nacional aplicable para poder determinar los elementos que serán esenciales en este análisis. Por tanto, pese a resaltar el carácter de concepto autónomo de la definición de responsable, de nuevo el GA29 remite a la legislación nacional para interpretar uno de los aspectos determinantes del alcance del

[217] Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.* pág. 15.
[218] *Ibídem.*
[219] *Ibídem.*
[220] *Ibídem,* pág. 16.

concepto. Esta posibilidad de variación en el ámbito nacional socava la fortaleza del concepto.

Otra cuestión que cabe plantear es si es necesario que el sujeto ejerza efectivamente el poder de decisión sobre todos los aspectos (fines y medios esenciales), ya que su enunciado incluye una conjunción copulativa ("y"). Sin embargo, al haberse introducido la posibilidad de corresponsabilidad mediante el texto "solo o conjuntamente con otros" deja abierta la posibilidad a que se puedan determinar sólo parcialmente estos aspectos. En consecuencia, si el responsable no determina todos los aspectos es porque puede ser que otro lo haga y se trate de un supuesto de corresponsabilidad.

Por otro lado, si el encargado del tratamiento decidiera sobre un medio considerado esencial (p. ej. qué terceros podrán acceder a los datos) ¿podría considerarse que este encargado se convierte en responsable o es preciso que determine todos los medios considerados esenciales y los fines del tratamiento para calificarlo en este sentido? Entiendo que, tanto si determinara los fines, como parte esencial de los medios, este sujeto deberá considerarse responsable. Por tanto, debería haberse introducido una conjunción disyuntiva "o", para indicar que el responsable será quien determinará los fines "o" los medios del tratamiento.

2.3.2. El origen de la capacidad de determinación del responsable

Para identificar si un responsable tiene poder de determinación sobre los fines o medios del tratamiento de datos, se puede acudir a la fuente de ese poder. De esta forma, cuando se identifique la fuente querrá decir que existe el poder de determinar y se cumplirá con el elemento funcional del concepto de responsable del tratamiento. Este es el método por el que opta el GA29, que ofrece tres posibles categorías de situaciones de acuerdo con la fuente de la que emana este poder de determinación, categorías que se presentan a continuación[221]. No obstante, si bien se hará referencia a esta clasificación, hay que advertir que no resulta todo lo clara que se pretendía.

[221] Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.* pág. 11.

a. El poder de determinación emana de una competencia legal explícita

En este apartado haré referencia a aquella categoría de situaciones en las que el poder de determinación del responsable emana de una competencia legal explícita. Este sería, por ejemplo, el caso al que hace referencia la última parte de la definición de responsable de tratamiento en la que se indica que "en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario" (art. 2.d) Directiva 95/46/CE).

Como se ha indicado en el análisis relativo al concepto de responsable en el Convenio 108, en este texto se realizaba una remisión a las leyes nacionales para determinar si la "autoridad controladora del fichero" era competente para decidir sobre el objeto. También se apuntaba a que el Informe explicativo precisaba que estas leyes a las que se remitía el Convenio 108 eran las leyes de protección de datos nacionales[222].

En la Propuesta de Directiva de 1990 se recogió, de forma similar al Convenio 108, una remisión al derecho comunitario o a la legislación del Estado miembro para establecer la competencia del responsable para decidir. Este reenvío se eliminó de la definición del texto de 1992, pero se retomó en el texto final de la Directiva 95/46/CE. Sin embargo, en la versión definitiva de la directiva se modificó sustancialmente el texto inicial. Por un lado, la identificación del responsable se realiza en virtud de su capacidad de determinar, sin tener que acudir a ninguna ley para ello. No obstante, se introduce el reenvío para los casos en los que el legislador quiera indicar quién considera adecuado que sea el responsable de un tratamiento, respecto al tratamiento que regule.

En virtud de esta variación en el concepto, el GA29 interpreta que se podrá calificar a un responsable del tratamiento como tal, independientemente de que la ley le otorgue la competencia para tratar datos[223]. Esta remisión optativa acarrea, según el GA29, que la noción de responsable del tratamiento se convierta en un concepto

[222] Ver Capítulo I.
[223] Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.*, pág. 9.

comunitario autónomo, no sujeto a las divergencias que puedan existir en las legislaciones nacionales de protección de datos y en un concepto autónomo independiente de las calificaciones de responsabilidad de otras leyes sectoriales[224].

En el texto final, el reenvío no persigue que la legislación señale cuándo el responsable es competente para decidir y, por lo tanto, de hallar en ella la única fuente para saber quién será responsable. Esta remisión a la ley se debe entender como una consecuencia natural derivada de la previsión por esta ley de un tratamiento de datos personales. Cuando, en esos casos, la ley establezca los fines y los medios del tratamiento, también podrá sumar la determinación de quién será el responsable o los criterios que contribuyan a su determinación.

De entrada, si nos limitamos a la interpretación literal de la norma, la ley deberá fijar estos dos elementos (fines y medios) como requisito para poder determinar el responsable. Además esta capacidad de determinación se configura como una potestad del legislador. De nuevo, entiendo que debería interpretarse que la ley podrá establecer los fines o los medios del tratamiento para poder incluir quien es el responsable. No será preciso que deba determinarse los fines y los medios.

El GA29 parece deducir que, pese a que la Directiva 95/46/CE se remita al legislador nacional o comunitario para la designación o fijación de los criterios, no es que deje en manos de este legislador la posibilidad de modificar las características del concepto del responsable[225]. Y es que, al ser la noción de responsable un concepto autónomo de derecho comunitario, exige de una interpretación uniforme, no sujeto a las variaciones de las leyes nacionales. Lo que deja en manos del legislador sería la designación formal del responsable como algo natural al definir la necesidad de llevar a cabo un tratamiento. Sin embargo, el legislador deberá realizar esta designación mediante la aplicación de los elementos del concepto. De otra manera, podrían existir conflictos entre la designación legal y la aplicación del concepto, a lo que se hará referencia más adelante.

[224] *Ibídem.*
[225] *Ibídem.*

Por lo tanto, como se ha indicado, en esta categoría se incluirían aquellos supuestos en los que, en la legislación se realiza el nombramiento expreso del responsable del tratamiento o se fijan estos criterios específicos para llevar a cabo este nombramiento, lo que, en definitiva, no sería muy frecuente[226]. Por eso, el GA29 también se refiere a la posibilidad, más frecuente en la práctica, de que la legislación lo que haga sea imponer un cometido o una responsabilidad que implique tratar datos[227]. De esta imposición del cometido o responsabilidad se deducirá que existe un poder de determinación por parte del responsable.

b. El poder de determinación emana de una competencia implícita

El segundo supuesto que el GA29 establece es el del control que emana de una competencia implícita[228]. En este caso, no se establece en leyes de forma explícita, sino que emana de normas jurídicas comunes o de la práctica jurídica en ámbitos como el derecho civil, laboral o mercantil[229]. De esta forma, la capacidad para determinar estaría fuertemente vinculada con las funciones y obligaciones que deben llevar a cabo estos sujetos, de acuerdo con su regulación.

Cuesta diferenciar este supuesto del que indicábamos anteriormente, en el que se entendía como control emanado de una competencia legal explícita, la asignación de un cometido que necesariamente implicará el tratamiento de datos. En todo caso, la diferencia sería sutil, ya que en el caso de la competencia legal explícita hay que entender que el cometido está expresamente descrito y junto a él, también se describe que se tendrán que tratar determinados datos. En la competencia implícita se deduce que ésta no estará expresamente incluida en una ley, sino que se deriva de atribuciones, competencias, funciones que sí estarían establecidas en una ley. Lo que no figuraría

[226] *Ibídem.*
[227] *Ibídem.*
[228] En la versión en español del dictamen del GA29 se indica "control emanado de una competencia jurídica implícita". Sin embargo, en la versión en inglés no se incluye el término "jurídica", de forma que se alude al "*control stemming from implicit competence*". *Opinion 1/2010 on the concept of "controller" and "processor", 00264/10/EN WP 169, 16.2.2010, Article 29 Data Protection Working Party*, pág. 10.
[229] En este caso el GA29 cita como ejemplo que si la legislación laboral establece que el empleador debe cumplir una serie de obligaciones respecto a sus empleados, como el pago de sus salarios, esto implicará que este empleador deba tratar datos personales en calidad de responsable del tratamiento. Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.* pág. 11.

expresamente en esta ley es que estas atribuciones, competencias o funciones implicaran un tratamiento de datos personales[230].

El GA29 menciona el Considerando 47 Directiva 95/46/CE, como ejemplo de orientación jurídica, proporcionada por el legislador comunitario, sobre quién debería ser calificado como responsable en un determinado contexto[231]. Entiendo que el GA29 alude a este crietrio como ejemplo de un supuesto de competencia implícita porque es una orientación y no una competencia legal explícita.

Según este Considerando 47 Directiva 95/46/CE se considera que los operadores de telecomunicaciones (o proveedores de comunicaciones electrónicas como se denominan actualmente), normalmente sólo deberán considerarse responsables del tratamiento de los datos sobre el tráfico y la facturación de sus abonados, pero no de los datos transmitidos, de los que será responsable la persona que realiza la transmisión. Esta aclaración se incluyó en la Directiva 95/46/CE, aunque su lugar hubiera debido ser la posterior Directiva 97/66/CE, que regularía la protección de datos en el sector de las telecomunicaciones[232].

Pese a que el operador tenga una competencia atribuida, consistente en transmitir datos, no se le considera responsable del tratamiento porque esta competencia no implica que tenga capacidad de control sobre esos datos. Así, este proveedor no es ni el que inicia la comunicación ni el que selecciona el destinatario ni el que modifica la información, por

[230] De esta forma en el ejemplo que citaba el GA29 relativo al empleador, el pago de salarios es una obligación legal pero sería una competencia jurídica implícita si en la ley no se especificara por ejemplo que "para realizar el pago de salarios el empleador deberá solicitar a sus empleados sus datos bancarios". *Ibídem.*

[231] El Considerando 47 de la Directiva 95/46/CE establece: "Considerando que cuando un mensaje con datos personales sea transmitido a través de un servicio de telecomunicaciones o de correo electrónico cuyo único objetivo sea transmitir mensajes de ese tipo, será considerada normalmente responsable del tratamiento de los datos personales presentes en el mensaje aquella persona de quien proceda el mensaje y no la que ofrezca el servicio de transmisión; que, no obstante, las personas que ofrezcan estos servicios normalmente serán consideradas responsables del tratamiento de los datos personales complementarios y necesarios para el funcionamiento del servicio;". Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.* pág.12.

[232] Este considerando aparece aprobado en la Posición común (CE) nº1/95 adoptada por el Consejo el 20.2.1995 con vistas a la adopción de la Directiva 95/…/CE del Parlamento Europeo y del Consejo, de …, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO C 93 de 13.4.1995. Hay que tener en cuenta que los textos de las dos directivas, la Directiva 95/46/CE y la Directiva 97/66/CE (que luego se convirtió en la Directiva 2002/58/CE), se elaboraron al mismo tiempo, si bien después se retrasó aún más la aprobación de esta última. Por tanto, la introducción de este considerando pudo deberse a la necesidad de aclarar esta cuestión y no esperar a la aprobación de esta directiva específica.

lo que no decide los fines ni los medios del tratamiento[233]. Estos criterios que se utilizan para establecer que los operadores de telecomunicaciones no son responsables, son los mismos que introdujo la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) (Directiva 2000/31/CE) para excluir la responsabilidad de estos sujetos, respecto a los contenidos que transmiten.

Pero, si el operador no se considera responsable del tratamiento, cabe cuestionarse ¿no debería ser considerado encargado del tratamiento? ¿Es necesario que un sujeto que trata datos personales encaje en uno de estos dos roles: responsable o encargado?

Un proveedor de servicios de comunicaciones electrónicas que presta un servicio de transmisión de datos, ya sea un servicio telefónico, o un servicio de conexión a Internet, lleva a cabo un tratamiento de datos de carácter personal, ya que se puede decir que, como mínimo, realiza una comunicación por transmisión de estos datos[234].

En el ámbito comunitario, hay otra norma comunitaria que regula específicamente las obligaciones de estos proveedores, en materia de protección de datos: la Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (Directiva 2002/58/CE). En esta directiva no se identifica ningún criterio que nos ayude a clarificar si este proveedor podría ser calificado como encargado del tratamiento respecto a los datos transmitidos. Más bien, lo que hace esta norma es asumir que estamos ante un responsable del tratamiento, si bien es verdad que su regulación se centra en aquellos tratamientos de datos respecto a los que el Considerando 47 apuntaba que el proveedor era responsable del tratamiento. Respecto a los datos transmitidos

[233] Según el GA29 una autoridad de control tuvo que dilucidar si un operador de telecomunicaciones era responsable. Un interesado denunció que recibía comunicaciones comerciales no solicitadas a través del correo electrónico y solicitó al operador que le confirmara o le negara que era el remitente de estas comunicaciones. La autoridad de control concluyó que el operador sólo facilita al cliente el acceso a una red de comunicación, no inicia la transmisión de datos ni selecciona a los destinatarios ni modifica la información transmitida. Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.* pág. 12.

[234] Esta es una de las operaciones que se consideran tratamiento de datos personales según la definición contenida en el artículo 2.b) Directiva 95/46/CE.

contempla la obligación de adoptar medidas para garantizar la confidencialidad y la seguridad (arts. 4 y 5 Directiva 2002/58/CE).

Esta norma se remite a la Directiva 95/46/CE para la aplicación de las definiciones, así como para todas las cuestiones que, en esta materia, no estén cubiertas específicamente por la Directiva 2002/58/CE y se mencionan expresamente las obligaciones del responsable del tratamiento (Considerando 10 Directiva 2002/58/CE). Además, se aclara que la Directiva 95/46/CE se aplica a los servicios de comunicaciones electrónicas que no sean de carácter público.

Si el objetivo de la regulación es asegurar una efectiva asignación de responsabilidades, debe tenerse en cuenta a la hora de configurar el concepto de las figuras de responsable y encargado. En cualquier tratamiento de datos personales que se efectúe debería poder hallarse el responsable que está detrás del mismo. Si en este caso, es el emisor de los datos, hay que plantear si el proveedor del servicio de transmisión debe considerarse un encargado del tratamiento.

Llama la atención que, respecto a un proveedor de servicio de correo electrónico de carácter privado, el GA29 sí entiende que estamos ante un encargado del tratamiento, cuando el Considerando 47 se refiere indistintamente a servicios de telecomunicaciones o de correo electrónico[235]. ¿Por qué parece que está claro que un proveedor de servicios de correo electrónico es encargado del tratamiento y no que lo sea un proveedor de servicios de comunicaciones electrónicas como el telefónico?

Entiendo que los prestadores de servicios de comunicaciones electrónicas públicos están sometidos a una fuerte regulación y que la información que transmiten se protege mediante otras vías, como el derecho al secreto de las comunicaciones. Precisamente la protección de este derecho al secreto de las comunicaciones es el mejor argumento para entender que no puede ser considerado responsable del tratamiento, ya que no puede ni utilizar ni alterar esos datos. Sin embargo ¿esto es motivo de que no se aplique la figura del encargado? La respuesta es que en este sector relativo a los servicios de comunicaciones electrónicas, el legislador ha estimado que quedaban definidos los

[235] Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.* pág. 29, ejemplo nº 18.

sujetos obligados y que los datos objeto de transmisión recibían una adecuada protección. Tampoco parece viable que los usuarios de estos servicios, actuando como responsables, pudieran dar instrucciones a estos prestadores (aparte de las de envío y recepción de la información transmitida) y tener el control, por ejemplo, sobre las subcontrataciones que efectuaran los mismos. Además, a esto hay que sumar que el ámbito de protección de esta normativa específica es más amplio que el de la Directiva 95/46/CE, ya que también protege a las personas jurídicas.

En conclusión, en el ámbito de los prestadores de servicios de comunicaciones electrónicas se ha optado por una regulación específica y, pese a que remite a la regulación general en materia de definiciones y obligaciones, se ha considerado que no deben aplicarse los conceptos de responsable y encargado, respecto a los datos transmitidos.

La falta de asignación de un rol, si bien se compensa por la protección de una regulación más estricta en materia de seguridad de los datos, resta coherencia al marco regulador general del derecho a la protección de datos, que debería exigir la calificación de todos los que realizan tratamientos de datos en alguna de las figuras que se han configurado, con el objetivo de mantener un control de todo el ciclo del tratamiento de datos.

Una muestra de la inseguridad que puede crear esta falta de coherencia es la sentencia del TJUE *Probst* que planteaba el rol que ostentaba un cesionario de créditos al que un prestador de servicios de comunicaciones electrónicas había proporcionado datos de tráfico, con el fin de que gestionara el cobro de estos impagados[236]. La Directiva 2002/58/CE permite que estos prestadores utilicen los datos de tráfico a efectos de facturación y exigencia de pago (art. 6.2 Directiva 2002/58/CE). Asimismo, se establece que pueda encargarse el tratamiento de estos datos, para esta finalidad, a personas que actúen bajo la autoridad del proveedor (art. 6.5 Directiva 2002/58/CE).

Como el TJUE no encuentra ningún argumento en los trabajos preparatorios de la Directiva 2002/58/CE para interpretar qué debe entenderse por "personas que actúen bajo

[236] Sentencia del TJUE de 22 de noviembre de 2012 *Probst*, C-119/12, EU:C:2012:748.

la autoridad del proveedor", acude a otras disposiciones similares de la Directiva 95/46/CE, que estima son los artículos 16 y 17 Directiva 95/46/CE, en los que se especifica el nivel de control que el responsable ejercerá sobre el encargado del tratamiento[237].

El TJUE considera que, si del contrato suscrito entre el prestador de servicios y el cesionario de créditos, se deduce que permite ese control por parte del prestador, se podrá estimar que el cesionario actúa bajo la autoridad del prestador[238]. El tribunal europeo, en definitiva, lo que hace es encajar al cesionario en la figura de encargado del tratamiento. Sin embargo, la Directiva 95/46/CE considera que las personas que actúan bajo la autoridad del responsable son sujetos distintos al encargado, por lo que parece referirse a sujetos con una vinculación más directa, como la laboral[239]. El TJUE podría haber considerado que la Directiva 2002/58/CE también se refería a este tipo de sujetos y no a un encargado.

La referencia a personas que actúen bajo la autoridad del prestador debe entenderse que incluye a los encargados del tratamiento, aunque la Directiva 2002/58/CE debería haber hecho referencia expresa a los mismos. Y es que la misma Directiva 2002/58/CE indica que, si el proveedor de servicios subcontrata el tratamiento de datos personales necesario para la prestación de dichos servicio a otra entidad, dicha subcontratación y el tratamiento de datos deben cumplir los requisitos relativos a los responsables y a los encargados del tratamiento que establece la Directiva 95/46/CE (Considerando 32 Directiva 2002/58/CE).

Lo que, al final se concluye de esta sentencia, es que el TJUE entiende que el cesionario es un encargado, sin calificarlo expresamente como tal y en función de unos términos, que en la Directiva 95/46/CE, a la que acude, hacen referencia a otro tipo de

[237] *Ibídem*, apdos. 20 y 25.
[238] *Ibídem*, apdos. 27 a 30.
[239] Así se deduce de la definición de tercero como "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento" y de la obligación de confidencialidad que tienen "las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento" (arts. 2.f) y 16 Directiva 95/46/CE).

sujetos. Esto se traduce en una confusión en la aplicación de los conceptos y en falta de claridad para los responsables que tengan que aplicarlos.

Respecto a la orientación que proporciona el Considerando 47 Directiva 95/46/CE también hay que mencionar la sentencia del TJUE en el asunto *Google.* En la misma se cuestionó si un servicio de búsquedas de páginas web podía considerarse responsable del tratamiento respecto a los datos personales que se encuentran en las páginas web a las que se enlaza, a lo que se respondió afirmativamente[240]. En este caso, también se argumentó que el buscador no tenía control sobre los datos y, precisamente, se alegó el Considerando 47 Directiva 95/46/CE. Me remito, no obstante, al análisis más detallado que realizo de este pronunciamiento posteriormente[241].

Es importante tener presente que el hecho de calificar a un determinado sujeto como responsable tiene importantes consecuencias. Estimo que es necesario poder atribuir a todos los sujetos implicados en un tratamiento de datos uno de los papeles asignados por la regulación, mediante las definiciones. Ante una regulación específica sectorial debería quedar claro el rol asignado en virtud de la legislación general. Si el sector exige que se modifique el rol o que no se pueda aplicar, debería clarificarse, con el fin de proporcionar seguridad jurídica tanto para los responsables, como para las autoridades, órganos judiciales y titulares de datos.

c. El poder de determinación emana de una capacidad de influencia de hecho

El tercer supuesto que señala el GA29 es cuando el control emana de una capacidad de influencia de hecho. Lo que deberá analizarse, en este caso, para poder establecer la capacidad de determinación del sujeto son las circunstancias de hecho. Esto supondrá en la mayoría de los casos, el análisis de las relaciones contractuales entre las partes[242].

[240] Sentencia del TJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González,* C-131/12, EU:C:2014:317.
[241] Ver Capítulo VIII.
[242] Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.* pág. 12.

De la misma manera que el GA29 diferenciaba en los dos supuestos anteriores el control que emana de forma explícita o de forma implícita de la legislación, considero necesario hacer aquí también esta diferenciación. En muchas ocasiones, esto responderá a si el sujeto objeto de análisis ha realizado o no la adaptación de su organización a la regulación de protección de datos. Y es que si se ha realizado esta adaptación, lo habitual es que tenga reflejo en los contratos o en documentos contractuales que se utilicen para cumplir con las obligaciones de la legislación de protección de datos (p.ej. en los documentos que utilice para cumplir con el deber de informar). En consecuencia, se indicará explícitamente en estos documentos si el sujeto se considera responsable del tratamiento.

Si, por el contrario, no se ha llevado a cabo la adaptación a la legislación, no se contará con esta documentación y, por lo tanto, sólo restará limitarse al análisis del supuesto de hecho. No obstante, también pueden existir contratos que sí den información que ayude a determinar si el sujeto tiene esta capacidad de determinación. De la misma forma que en la legislación se puede encontrar la información necesaria para conocer las obligaciones que implican tratamientos de datos y la necesidad de que ese tratamiento lo determine un preciso sujeto, también esta información se puede hallar en los contratos.

d. Conflictos entre la designación formal y la influencia de hecho

Si bien el GA29 manifiesta que las dos primeras categorías permitirán identificar con mayor seguridad al organismo que se considerará responsable del tratamiento, apunta que la designación legal formal deberá estar en consonancia con la realidad de los hechos[243]. Entonces ¿qué sucederá en el caso de que una ley designe explícitamente a un sujeto como responsable del tratamiento y la realidad apunte a que ese sujeto no cuente con ese poder de determinación efectiva? Pues parece que el GA29 se decanta por primar la realidad sobre la previsión legal[244], por lo que estaríamos ante un conflicto. Debería darse siempre prevalencia a la realidad, a quién tiene la capacidad de control sobre el tratamiento de datos.

[243] Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.* pág. 13.
[244] *Ibídem.*

En consecuencia, se podría plantear si ¿era necesario hacer referencia a la posibilidad de que el legislador designara al responsable si establecía los fines y los medios del tratamiento? Si se interpreta que debe prevalecer la realidad en lo que respecta al juicio sobre el poder de determinación que tiene el responsable sobre los fines y los medios del tratamiento, la única conclusión que cabe es la de entender que el reenvío es superfluo y lo único que hace es añadir confusión al concepto. El reenvío sólo tendría sentido si se decidiera dar un margen de maniobra a los Estados miembros para modificar los criterios de determinación del responsable, criterios que afectarían a los elementos del mismo y que permitirían, por ejemplo, una designación meramente formal, que podría no corresponder con la realidad. Igualmente podría ser útil a efectos de clarificar a los sujetos afectados su papel, pero esto supondría que ese papel esté claro y que tenga un carácter permanente, lo que parece corresponder, en principio, al sector público. En este sector tendrá más sentido asignar el papel, en un entorno en el que existe una organización más perfilada.

Evidentemente el legislador debe fijar normas que implicarán tratamientos de datos que deberán llevar a cabo sujetos obligados por estas normas. Esto enlazaría con la legitimación de los responsables para tratar datos personales, cuando así se lo exige una ley[245]. Sin embargo, no siempre que una norma prevea que un sujeto deba tratar datos personales, obliga a que ese sujeto siempre tenga que ser calificado de responsable, ya que, como veremos, también podrá ser un encargado del tratamiento.

En lo que respecta a la tercera categoría, en la que el poder de determinación se origina en la capacidad de influencia de hecho del responsable, como se ha indicado, supondría analizar los documentos contractuales existentes en algunos casos. No obstante, como sostiene el GA29, pese a contar con contratos que puedan permitir esta designación del responsable, esta documentación no siempre será determinante[246]. Las partes podrían designar al responsable en función de sus intereses, sin atender realmente a quién ostenta

[245] Recordar en este sentido el Considerando 32 Directiva 95/46/CE que establece que es la legislación nacional a la que corresponde determinar si el responsable del tratamiento que tiene conferida una misión de interés público o inherente al ejercicio del poder público, debe ser una administración pública u otra persona del derecho público o privado, como una asociación profesional.

[246] Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.* pág.12.

el verdadero control sobre los datos[247]. Por tanto, el análisis no debe limitarse a esta documentación, sino que hay que ir más allá.

Hay que tener en cuenta que el GA29 está formado por las diferentes autoridades de protección de datos europeas. En sus dictámenes reflejan su práctica diaria. Por lo tanto, su perspectiva es la del analista que se enfrenta, como he indicado, a una estrategia jurídica adoptada por el responsable del tratamiento con relación al cumplimiento de la legislación de protección de datos, o a veces, a la ausencia de ella. Por lo tanto, lo que plantea el GA29 es la postura que debe seguir dicho analista y le conmina a ir más allá de la documentación preparada por el responsable del tratamiento y analizar las verdaderas circunstancias del supuesto de hecho. Las autoridades de control cuando deben valorar si un sujeto no cumple con lo establecido en la normativa, por encima de todo estudiarán estas circunstancias.

Como criterios que pueden servir de ayuda, al margen de las condiciones contractuales mencionadas, el GA29 cita el grado de control real ejercido por una parte, la imagen dada a los interesados o las expectativas razonables de los interesados sobre la base de esta visibilidad[248].

El primer criterio relativo al grado de control real entiendo que no es más que atender a quién tiene la capacidad de determinación, en virtud de los elementos fácticos.

[247] Como ejemplo de esto se puede citar el asunto SWIFT, analizado por el GA29 en uno de sus dictámenes. Este asunto se conoció a través de los medios de comunicación en julio de 2006. En ese momento se divulgó que la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (*Worldwide Interbank Financial Telecommunication*-SWIFT) había proporcionado desde finales del año 2001 datos personales de las transferencias de dinero realizadas a través de la red SWIFT a la Oficina de Control de Activos Extranjeros (*Office of Foreign Assets Control-OFAC)* del Departamento del Tesoro de los Estados Unidos (*UST*) en respuesta a citaciones realizadas en virtud de la legislación estadounidense a efectos de la investigación sobre el terrorismo. SWIFT era una cooperativa domiciliada en Bélgica que se dedicaba a prestar un servicio de mensajería financiera a más de 7.800 entidades financieras de todo el mundo. Tras realizar una investigación de este servicio, la autoridad de control belga llego a la conclusión que SWIFT incumplía con la legislación de protección de datos. Pues bien, el GA29 indica que, pese a la relación contractual existente entre SWIFT y las entidades financieras conforme al derecho civil o mercantil que pueden configurar a esta empresa como subcontratista, respecto a la legislación de protección de datos no podía considerarse que SWIFT fuera un encargado del tratamiento. Del examen, tanto de la gestión que realizaba esta cooperativa en el uso normal de los datos, como en las transferencias de datos al UST, el GA29 concluye que actuó con autonomía respecto a las entidades financieras y determinó los fines y los medios del tratamiento, por lo que debía considerase que era un responsable del tratamiento. Dictamen 10/2006 sobre el tratamiento de datos personales por parte de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (*Worldwide Interbank Financial Telecommunication*-SWIFT), 01935/06/ES WP 128, 22.11.2006, Grupo de trabajo Artículo 29 sobre la protección de datos, págs. 13 a 14.

[248] Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.* pág. 13.

No es pues nada diferente de lo ya comentado anteriormente. En cuanto a los otros dos criterios son ejemplo de que se quiere primar la protección de los interesados. Y es que con estos criterios se olvida la situación real y se acude a una percepción subjetiva de los interesados. No hay que olvidar que los interesados, pese a ser los sujetos afectados, son parte ajena a la determinación de quien lleva a cabo el tratamiento.

Pese a que estos criterios protejan al máximo a estos afectados, entiendo que no se pueden poner por encima de la realidad. Más bien se deben tomar como indicios que ayuden a la determinación del responsable. Las autoridades de control no deberían conformarse con este dato que pueden obtener fácilmente y profundizar en la situación de hecho.

Por último, cabe señalar la consecuencia de no poder aplicar ninguna de las categorías señaladas por el GA29. Según indica el GA29 estaríamos ante la nulidad de pleno derecho de la designación de responsable del tratamiento[249]. Es decir, si el poder de control del sujeto analizado no emana de ninguna de las fuentes indicadas, lo único que resta concluir es que no tiene poder de control sobre el tratamiento y, por tanto, si se le ha identificado como responsable, esta determinación no ha sido correcta. Por ello, la designación debe considerarse nula, lo que implicará entonces examinar si se han cometido infracciones de la normativa de protección de datos.

También es interesante apuntar que el análisis del origen del poder de determinación del responsable nos ayudará más tarde a establecer su legitimación, necesaria para poder realizar el tratamiento. No hay que olvidar que estamos en el estadio en el que analizamos si el sujeto que trata datos puede considerarse responsable del tratamiento o no. Una vez se determina que estamos ante un responsable del tratamiento, hay que analizar si este sujeto puede tratar datos personales y si cumple con todas las obligaciones que, como veremos más adelante, conforman su estatuto.

Asimismo, puede ser que se considere que un responsable tiene poder de determinación sobre los fines y medios de un tratamiento y que no cuente con esta legitimación para tratar datos. Precisamente porque se estaría en este primer estadio que

[249] *Ibídem.*

lo que pretende es asegurar la asignación de responsabilidades, independientemente de la licitud del tratamiento o de la designación formal del responsable. De esta forma, un responsable que no hubiera sido designado de acuerdo con los requisitos formales establecidos o que realizara un tratamiento sin tener legitimación para ello, podrá ser considerado responsable del tratamiento y, por tanto, responder en virtud de la legislación de protección de datos[250].

2.3.3. Corresponsabilidad

La mención "solo o conjuntamente con otros" fue introducida en el proceso legislativo, en el último momento, por el Parlamento Europeo[251]. La Comisión parlamentaria que lo introdujo pretendía cubrir aquellos supuestos en los que varias personas actuaran con una finalidad determinada y se dotaran de medios técnicos para ello, sin encuadrarse en el marco de una persona jurídica. Del mismo modo se aludía a la posibilidad de cubrir intercambios de información entre administraciones y empresas en el marco de redes digitales[252]. No podían prever los miembros de esta Comisión la importancia que adquirirían esos intercambios digitales de información.

Cuando se introdujo, se pensaba en que las diferentes partes determinaran conjuntamente los fines y los medios respecto a una única operación. Por tanto, no se

[250] Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.* págs. 9 a 10.

[251] Decisión del Parlamento sobre la posición común del Consejo respecto de una Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO C 166 de 3.7.1995.

[252] Para entender porque se introdujo hay que acudir a un dictamen de la Comisión de asuntos económicos y monetarios y de política industrial del Parlamento Europeo, que es la que propone el cambio e indica concretamente: "La letra d) del artículo 2 es importante puesto que permite determinar la persona a la que incumbirán las obligaciones previstas en la directiva. El texto parece contemplar sólo la situación, que ciertamente es la más corriente, de que no haya más que una única persona considerada responsable. Sin embargo, en la práctica, es posible que varias personas decidan efectuar un tratamiento de datos personales para una finalidad determinada o en el marco de unas relaciones permanentes (por ejemplo, en el seno de un grupo cooperativo o de una asociación profesional) y decidan asimismo dotarse de medios técnicos con este fin. En este caso, cada una de estas personas, en la medida en que no actúen en el marco jurídico de una persona jurídica, debería ser considerada corresponsable. Esta situación podría darse cada vez con más frecuencia en el futuro, en particular, en caso de intercambios de información entre administraciones o entre empresas en el marco de redes telemáticas. En estas situaciones, las personas podrían tener dificultades para actuar contra uno y otro de los responsables si el texto no es lo suficientemente claro." Recomendación para la segunda lectura sobre la posición común adoptada por el Consejo con vistas a la adopción de una Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, Comisión de asuntos jurídicos y de derechos de los ciudadanos, 24.5.1995, PE 212.057/def, que, en anexo, incluye la Opinión de la Comisión de asuntos económicos y monetarios y de política industrial, 24.5.1995.

reflejaba la complejidad de los supuestos de corresponsabilidad que pueden plantearse. La participación de las partes en la determinación conjunta puede revestir distintas formas y el reparto no tiene que ser necesariamente a partes iguales[253]. Los diversos sujetos pueden tener una relación muy estrecha y compartir todos los fines o medios del tratamiento, o una relación más laxa, al compartir sólo los fines o los medios, o una parte de éstos[254]. Así, según el GA29 "conjuntamente" significa "junto con otros" o "no solo"[255] y no excluye la posibilidad de que distintos agentes estén implicados en diferentes operaciones de un mismo tratamiento[256]. Estas operaciones pueden producirse simultáneamente o en distintas fases.

Así, el GA29 define control conjunto como aquella situación en la que diferentes partes determinan, respecto a unas operaciones de tratamiento específicas, o bien los fines, o bien aquellos elementos esenciales de los medios que caracterizan al responsable del tratamiento[257]. Para evaluar el control conjunto se deberán seguir los mismos criterios que para evaluar el control único[258].

En entornos tecnológicos hay situaciones de corresponsabilidad muy complejas en las que, en ocasiones, resulta complicado que algunos de los corresponsables cumplan con lo establecido en la legislación, debido a que pueden no tener contacto con los titulares de los datos[259]. En estos casos, es necesario que todos los que participen en el sistema cooperen para hacer posible el pleno cumplimiento de las obligaciones.

---

[253] Si de nuevo se retoma el asunto SWIFT, en el mismo el GA29 consideró, al evaluar la responsabilidad de SWIFT y la de las entidades financieras que eran clientes de esta cooperativa, que se trataba de un supuesto de control conjunto pero indicó que ello no implicaba que esa responsabilidad fuera igual. De esta forma, mientras que consideró que SWIFT tenía una responsabilidad primaria del tratamiento de mensajería financiera, las entidades financieras asumían sólo responsabilidad del tratamiento de datos de sus clientes en el servicio. Como ejemplo, se indicaba que las entidades financieras aceptaban el marco contractual del servicio de mensajería y en el mismo se incluía que se realizaban las transferencias de datos personales supeditados a las citaciones dirigidas a las mismas entidades financieras o a SWIFT. Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.* págs. 15 a 16.

[254] *Ibídem,* pág. 21.

[255] *Ibídem,* pág. 19.

[256] *Ibídem,* págs. 19 a 20.

[257] *Ibídem,* pág. 21.

[258] *Ibídem,* pág. 20.

[259] Se pueden citar las plataformas de publicidad online donde existen diferentes sujetos implicados: la plataforma de publicidad que pone en contacto a editores que ofrecen espacios en sus sitios web para que aparezca publicidad de los anunciantes, que se citan como ejemplo nº 14. *Ibídem.* pág. 26. También puede mencionarse el desarrollo de aplicaciones para dispositivos móviles, que analiza el GA29 en uno de sus dictámenes. En este caso, los sujetos que participan son los desarrolladores de las aplicaciones, los fabricantes de los dispositivos, los que han desarrollado los sistemas operativos, las tiendas de aplicaciones y otros terceros, como pueden ser las plataformas de publicidad mencionadas que pueden incluir publicidad

El GA29, consciente de las dificultades en estos entornos, estima que puede otorgarse una cierta flexibilidad en este reparto de las obligaciones entre los corresponsables, siempre que se asegure el cumplimiento[260]. Por otro lado, en ocasiones, si todos los corresponsables cumplieran, por ejemplo, con la obligación de informar el afectado podría encontrarse con una multitud de informaciones que podrían hacerle más confuso el tratamiento cuando, en ocasiones ni siquiera será consciente de que existen todos estos responsables detrás. Lo mismo podría suceder si para ejercer los derechos que brinda la legislación, el titular de los datos tuviera que dirigirse a todos los corresponsables.

Estas situaciones entorpecerían el cumplimiento de la ley, que podría agilizarse, si cooperaran los corresponsables entre sí y ofrecieran al titular de los datos un punto de contacto o un aviso informativo con toda la información necesaria para conocer las distintas fases y sujetos que participan en el tratamiento. No obstante, el GA29 también recuerda que el reparto de las obligaciones debería reflejar la realidad del tratamiento subyacente[261].

Otra cuestión que se plantea es si el control conjunto implica siempre una responsabilidad solidaria. El artículo 23 Directiva 95/46/CE, que establece la regulación de la responsabilidad civil del responsable, utiliza el singular "responsable del tratamiento", por lo que apunta a este tipo de responsabilidad solidario[262]. No obstante, de nuevo, el GA29 entiende que los corresponsables podrán establecer una asignación

---

en estas aplicaciones o también proveedores de servicios de analítica o de servicios de comunicaciones. Entre todos estos sujetos se entablan flujos de datos personales del usuario de la aplicación. En muchas de las ocasiones, el usuario no es consciente de todo este vaivén de datos, ya que mucha de esta información se genera automáticamente, sin requerir una acción por parte del usuario. Dictamen 2/2013 sobre las aplicaciones de los dispositivos inteligentes, 00461/13/ES WP 202, 27.2.2013, Grupo de trabajo Artículo 29 sobre la protección de datos, págs. 11 a 16. Otro ejemplo es la llamada Internet de las cosas (*Internet of things*) que también analiza el GA29 en otro dictamen. El supuesto que se analiza es el relativo a la inclusión de sensores en objetos que se pueden utilizar de forma cotidiana, como pulseras, con el fin de que puedan volcar datos a Internet, como por ejemplo datos de la actividad deportiva del usuario. Para hacer esto posible intervienen una multitud de sujetos como los fabricantes de los objetos, redes sociales en las que los usuarios pueden compartir sus datos, los desarrolladores de las aplicaciones que permiten acceder a los datos que se recogen de los sensores o plataformas que sirven de intermediarios entre fabricantes y desarrolladores. *Opinion 8/2014 on the recent developments on the Internet of things, 14/EN WP 223, 16.9.2014, Article 29 Data Protection Working Party*, págs. 11 a 13.

[260] Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.*, pág. 26.

[261] *Ibídem.*

[262] *Ibídem.*

diferente de responsabilidad mientras se asegure que sea efectiva y que podrá repartirse entre los diferentes sujetos, si ello es posible, en virtud del examen de las circunstancias de hecho[263].

Estas situaciones de corresponsabilidad, que derivan de modelos de negocio eminentemente tecnológicos, tienen como consecuencia una gran dificultad de análisis. Los sujetos que intervienen, muchas veces, no son conscientes de las connotaciones jurídicas que conlleva el flujo de datos que entablan entre ellos. Habitualmente, algunos de los que participan están ubicados en países, en los que no deben tener en cuenta los requisitos legales en materia de protección de datos y, por lo tanto, se producen situaciones descompensadas, que ocasionan incumplimientos en cadena.

2.3.4. El poder de decisión como criterio prevalente sobre el de tratamiento efectivo

En la Propuesta de Directiva de 1992, además de que el responsable decidiera, también se añadió la necesidad de que tratara datos o que ordenara tratarlos. Por lo tanto, el responsable debía ser el tratador efectivo de los datos o el que ordenara a otro llevar a cabo este tratamiento. Este añadido se debió a que en este texto se incluyó la figura del encargado del tratamiento, que era el que trataba datos por cuenta del responsable. Esta referencia a que trate u ordene tratar se eliminó del texto definitivo, poniendo de relieve que lo importante era la decisión sobre los fines y los medios y no el hecho de realizar o no el tratamiento.

De esta forma, el tratador efectivo de los datos podrá ser el mismo responsable del tratamiento o el encargado del tratamiento o alguna de las personas autorizadas por alguno de estos dos sujetos. Las personas autorizadas por el responsable o el encargado del tratamiento deben estar bajo la autoridad directa, lo que parece apuntar a que debe tratarse de empleados y no podrían considerarse incluidas personas que puedan decidir como podrían ser profesionales o empresarios autónomos[264].

[263] *Ibídem,* págs. 25, 27.

[264] Hay que recordar que el requisito de que estén bajo la autoridad directa se puede extraer del concepto de "tercero" que lo define como "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento"(art. 2.f) Directiva 95/46/CE, el subrayado es de la autora).

Siempre que respeten el principio de sumisión a las instrucciones del responsable, el hecho de que estos otros agentes traten los datos no modificará la asignación de responsabilidad. Sin embargo, si alguno de estos agentes decidiera ir en contra de estas instrucciones, se convertiría en responsable del tratamiento y asumiría su responsabilidad como tal, respecto al tratamiento de datos. Esto sin perjuicio de la vía de escape que la regulación establece cuando esta "desobediencia" responda al cumplimiento de una obligación legal imperativa (art. 16 Directiva 95/46/CE) que comentaré a continuación.

Otra cuestión sería si el responsable podría ser considerado también infractor, por ejemplo, por no tener las debidas medidas de seguridad, que igual podrían haber evitado que el empleado llevara a cabo este mal uso de los datos.

2.4. Delimitación del concepto de responsable en contraposición con el del encargado del tratamiento

La Directiva 95/46/CE introdujo la figura del encargado del tratamiento que complementa la del responsable. En este apartado analizaré su concepto mediante su comparación con el de responsable para ver las características que los acercan y los alejan. Esta es una cuestión especialmente importante en la aplicación práctica de la legislación y que ampliaré cuando se aborde el análisis de la legislación nacional, especialmente la española.

Ya se explicaron las funciones del concepto de responsable que lo convertían en pieza clave de la regulación ¿Tiene el concepto de encargado esta relevancia?

El concepto de encargado del tratamiento en la Directiva 95/46/CE también permite que se le asignen obligaciones a un sujeto, aunque se centran en el cumplimiento de las medidas de seguridad y en seguir los dictados del responsable, como se comprobará en la parte dedicada al estatuto del responsable[265]. Asimismo, este concepto también sirve de criterio de aplicación de la ley, ya que las obligaciones relativas a las medidas de seguridad que deberá cumplir el encargado del tratamiento serán las que defina la legislación del Estado miembro en el que se establezca éste (art. 17 Directiva

[265]Ver Capítulos V y VI.

95/46/CE). Por tanto, en estos dos aspectos se asemejan ambos conceptos. No obstante, en lo que se refiere a la asignación de responsabilidades, la Directiva 95/46/CE sólo hace referencia al responsable, si bien, como se ha indicado nada obsta para que se pueda llevar a cabo esta asignación en la legislación nacional[266].

2.4.1. El análisis del concepto de encargado del tratamiento

El encargado del tratamiento no aparecía en el Convenio 108. Con esta figura se pretendía ampliar la protección de los tratamientos de datos de carácter personal que llevaban a cabo terceros por cuenta del responsable[267]. Se define en la Directiva 95/46/CE como "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento" (art. 2.e) Directiva 95/46/CE).

Si segmentamos el concepto en elementos, a semejanza del análisis seguido para el concepto de responsable, tendríamos un elemento subjetivo: "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo", un elemento objetivo: "datos personales" y un elemento funcional: "trate" "por cuenta del responsable del tratamiento". Además, también se incluye el elemento relativo a la pluralidad: "solo o conjuntamente con otros".

Con relación a los sujetos que pueden ser encargados del tratamiento, es decir, al elemento subjetivo, se asimila al concepto de responsable del tratamiento. Se repite la misma enumeración y también se trata de un concepto aplicable tanto al sector público como al privado.

El encargado debe ser una entidad diferenciada de la del responsable[268] y, por tanto, quedarían excluidas de este papel las personas que estén sometidas, por un vínculo

[266] Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.*, pág. 31. Como se verá en el Capítulo VII esto es lo que ha sucedido en la legislación española.
[267] El concepto se reconocía por primera vez en la primera propuesta de la Comisión con el fin de "evitar situaciones en las que el tratamiento por terceros por cuenta del responsable del tratamiento del fichero tenga el efecto de reducir el nivel de protección del que goza el interesado. *Ibídem*, pág. 27.
[268] *Ibídem.*

laboral al responsable, es decir, sus empleados[269]. Se considera que, al estar sometido el empleado al poder de dirección del responsable, no es preciso incluirlo ni en el concepto de responsable ni en el de encargado, ya que responderá el responsable.

El elemento objetivo se centra en los datos personales, unidad última del objeto del tratamiento. Sin embargo, al unirlo con el elemento funcional se puede decir que el objeto es el tratamiento de datos, verdadera razón de la existencia del encargo.

El elemento funcional, que es el que caracteriza a la figura, es la capacidad de tratar datos por cuenta del responsable del tratamiento. Por tanto, el encargado es un tratador efectivo que se define, en contraste con el concepto de responsable, por la carencia de poder de determinación. Lo que se busca, en definitiva, con este concepto es dejar clara la extensión de la responsabilidad del sujeto con el poder de determinación a ese tratamiento que lleva a cabo un tercero porque este sujeto así lo ha decidido. No obstante, como se verá, por ejemplo, en la legislación española, se ha optado por reforzar la protección y asignar también responsabilidad al encargado del tratamiento.

Al elegir al encargado, el responsable debe asegurarse de que reúna las garantías suficientes respecto a las medidas de seguridad a adoptar y además se debe asegurar de que el encargado cumple estas medidas (art. 17 Directiva 95/46/CE)[270]. La elección del responsable remite, por lo tanto, al concepto legal de delegación, siendo fundamental que el encargado del tratamiento cumpla con las instrucciones del responsable del tratamiento, al menos en lo relativo a los fines y a los elementos esenciales de los medios del tratamiento[271].

---

[269] Si bien SANTAMARÍA RAMOS entiende que la regulación establecida en la Directiva del encargado del tratamiento también admitiría su aplicación al empleado del responsable del tratamiento reconoce que no se ha acogido esta posible acepción regulando sólo lo que para este autor son otras dos acepciones de la definición de encargado de tratamiento: el que se refiere al outsourcing y el que se refiere al encargado de protección de datos (o más conocido por la denominación en inglés *Data Protection Officer*). Para este autor el empleado sería un encargado del tratamiento de segundo nivel. F. J. SANTAMARÍA RAMOS, *El encargado independiente. Figura clave para un nuevo derecho de protección de datos*, La Ley, Las Rozas (Madrid), 2011, págs. 41 a 50.

[270] Así el TJUE ha indicado que "de los artículos 16 y 17 de la Directiva 95/46/CE, en los cuales se especifica el nivel de control que ejercerá en cada caso el responsable del tratamiento sobre el encargado que seleccione, se desprende que este último sólo actuará cuando se lo encargue el responsable del tratamiento y que el responsable se asegurará de que se cumplan las medidas acordadas para proteger los datos personales contra cualquier tratamiento ilícito." Sentencia del TJUE de 22 de noviembre de 2012 *Probst*, C-119/12, EU:C:2012:748, apdo. 25.

[271] Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.*, pág. 28.

Y es que, en el análisis del concepto de responsable del tratamiento se indicaba que éste debía decidir sobre los fines necesariamente. Respecto a los medios el responsable debía decidir sobre los medios considerados esenciales, lo que dejaba un margen de decisión al encargado del tratamiento con relación a los medios no esenciales. Principalmente, se consideraba que estos medios no esenciales eran los medios técnicos y organizativos[272].

También hay que hacer referencia a la mención de "solo o conjuntamente con otros". Al igual que sucede con el responsable se admite que existan varios encargados del tratamiento que actúen a la vez. Pero, al contrario de lo que sucede con el responsable del tratamiento, donde la relación entre los corresponsables sería horizontal, en los casos de pluralidad de encargados lo normal es que la relación sea vertical[273]. De la misma forma, el GA29 ha considerado que es importante que las obligaciones y las responsabilidades se asignen con claridad y no se diluyan en la cadena de subcontratación[274].

Por último, hay que indicar que el encargado del tratamiento no es necesario que sea un sujeto que únicamente se dedique a realizar tratamientos por cuenta de un responsable del tratamiento o varios, sino que además puede también ostentar, al mismo tiempo, el papel de responsable[275].

[272] Si bien también se hacía la precisión de que para determinar si los medios técnicos no eran esenciales debía estarse a la legislación nacional que, en algunos casos, como en el español, establece obligaciones detalladas con relación las medidas de seguridad que implican que la decisión sobre la elección de las mismas sí sea esencial. *Ibídem.*

[273] Si bien se trata de una relación la de corresponsabilidad que, como ya se ha comentado anteriormente, es compleja y puede revestir diversas formas. En cuanto a la pluralidad de encargados del tratamiento también hay diversas opciones de estructura. Puede ser que el responsable contrate directamente con una pluralidad de encargados o puede ser que se trate de una cadena de subcontrataciones en la que un encargado del tratamiento subcontrate total o parcialmente a otra entidad para llevar a cabo el tratamiento, suponiendo, por lo tanto otro encargado del tratamiento. Se abordará esta cuestión más adelante. *Ibídem.* pág. 30.

[274] Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.*, pág. 31.

[275] Por ejemplo, el encargado podrá considerarse responsable respecto a los tratamientos de datos que lleve a cabo de sus propios empleados o de sus clientes. *Ibídem*, pág. 28.

2.4.2. La distinción entre responsable y encargado del tratamiento

Una cuestión esencial en materia de protección de datos será identificar si un sujeto al que un responsable le proporcione datos de carácter personal de otras personas es un responsable o un encargado del tratamiento[276]. Si en un primer momento podría parecer algo sencillo, en la práctica es algo enormemente complejo.

a. Si no es responsable ¿es encargado?

Aunque inicialmente se cumplan los elementos del concepto, lo difícil es delimitar si ese sujeto es un mero tratador efectivo de datos, que actúa sometido al responsable o si bajo esa apariencia se esconde un responsable que realmente tiene capacidad de determinar los fines y usos del tratamiento. Como se ha indicado, lo más fácil será averiguar si ese potencial encargado tiene un poder de determinación sobre los fines del tratamiento. Si el sujeto puede decidir sobre los fines, entonces, la conclusión debe ser que se trata de un responsable. En cambio, será más difícil cuando lo que se analice sea la determinación de los medios. Si son medios considerados esenciales debe calificarse al sujeto que los determine como responsable, en caso contrario podrá ser un encargado del tratamiento.

Evidentemente, para identificar si estamos ante un responsable se pueden utilizar los criterios apuntados anteriormente, que se centraban en hallar de dónde emanaba el poder de determinación. En caso de que no podamos identificar esta fuente de poder y si se dan los otros requisitos mencionados del concepto, podremos entender que estamos ante un encargado del tratamiento. Por tanto, la metodología, en este caso, será buscar si

[276] KUNER resalta que la distinción entre ambas figuras es esencial y cada vez más difícil de aplicar en la práctica debido al desarrollo tecnológico, de forma que los papeles pueden cambiar dependiendo del momento. Como el autor indica, las leyes nacionales se fundamentan en la caracterización de estos roles y si no hay una determinación clara es imposible que las partes sepan cuales son sus obligaciones. Habitualmente, las empresas se enzarzan en una batalla por determinar quien debe considerarse responsable o encargado y lo normal es que quieran ostentar el papel de encargado, ya que es el que tiene menos obligaciones y menor responsabilidad. Su recomendación es definir quién asume cada papel al inicio de la relación jurídica y articular los mecanismos necesarios para cumplir con lo establecido en la normativa aunque advierte que hay que huir de operaciones de maquillaje. C. KUNER, *European data protection law, corporate compliance and regulation*, 2nd ed., Oxford University Press, Oxford, 2007, págs. 71 a 73. CAREY también destaca la preferencia por las empresas en querer ser calificados como encargados del tratamiento y no responsables. Este autor comenta la Ley inglesa de protección de datos y explica esta preferencia porque las obligaciones que establece la ley están asignadas al responsable. P. CAREY, *Data protection. A practical guide to UK and EU Law*, 3rd ed., Oxford University Press, Oxford, 2009, pág. 211.

se está ante un responsable y, en caso de no ser así, buscar si se cumplen los elementos del concepto de encargado.

De nuevo cabe plantear la pregunta: ¿qué sucederá con un tratador efectivo de datos que no encaje en la figura de encargado del tratamiento ni en la de responsable y que tampoco sea una persona bajo la autoridad directa de responsable o encargado?[277] La seguridad jurídica, la amplitud y el objetivo de ambos conceptos deberían llevarnos a intentar encajar a todo tratador de datos en alguno de estos conceptos, ya que si no es así, puede dar lugar a lagunas en el cumplimiento[278].

b. La legislación como fuente de atribución de la condición de encargado

En referencia a estas fuentes de las que emana el poder de determinación, hay que recordar el reenvío que el concepto de responsable del tratamiento realizaba a la legislación en la que se determinasen los fines y los medios del tratamiento y que, podía también determinar el responsable. Pues bien, nada obsta a que también la legislación pueda establecer quien pueda considerarse encargado del tratamiento. Sin embargo, como ya apunté cuando me refería a esta posibilidad respecto al responsable, me parece arriesgado hacer esta designación, ya que se corre el riesgo de contradecir la realidad.

De la misma forma, en la normativa se pueden hallar las pistas para determinar si nos hallamos ante un responsable o un encargado. Cuando la normativa establece que debe realizarse un tratamiento puede también establecer quién debe llevarlo a cabo y si el tratador debe someterse a las instrucciones de otro sujeto o si es el que decidirá sobre éste. También se pueden hallar estas pistas en la práctica jurídica, del mismo modo que se

[277] También puede ser un tercero ajeno al círculo de influencia del responsable. No obstante, tal como hace la Directiva 95/46/CE, el tercero lo que hace es delimitar el supuesto de hecho al que se aplica la regulación. Las obligaciones se refieren a un tratamiento de datos sobre el que ejercerá su poder de determinación el responsable y que podrá encargar a otro sujeto (el encargado del tratamiento) o que podrán llevar a cabo personas a su cargo. Cuando proporcione los datos a un tercero será porque salen de su círculo de influencia y habrá que examinar ese nuevo ciclo para determinar quien será el nuevo responsable respecto al mismo.

[278] Así, por ejemplo, si se vuelve a la cuestión suscitada con el Considerando 47 Directiva 95/46/CE se ilustra la complejidad de la determinación de responsable y encargado del tratamiento. Lo ideal será encajar al prestador de servicios de comunicaciones electrónicas en el papel del encargado del tratamiento. Sin embargo, pueden crearse situaciones en las que sea difícil y se pierda la conexión jurídica entre el usuario y el operador. Entiendo que en estos casos, la legislación suple esta protección, como sucede con la legislación aplicable al sector de las telecomunicaciones.

puede hallar si existe un poder de control que emane de una competencia implícita, como sucedía en el caso del responsable.

Es interesante mencionar la superposición de regulaciones a las que se podrá ver sometido el encargado. Por un lado, deberá llevar a cabo su actividad empresarial o administrativa, siguiendo lo preceptuado en la normativa que pueda existir y que regule esta actividad. Por otro lado, de acuerdo con la normativa de protección de datos deberá atender a las instrucciones del responsable si esa actividad que ejerce el encargado incluye el necesario tratamiento de datos para ese responsable. Esta cuestión implica que exista una tensión entre ambas regulaciones que, a veces, puede implicar que deba considerarse responsable a un sujeto que, inicialmente, podría parecer encargado del tratamiento. La razón es que estas obligaciones legales pueden comportar que este aparente encargado deba gozar de una cierta autonomía con relación al responsable. Esta autonomía ya no sólo puede deducirse de las obligaciones legales, sino de obligaciones que pueden ir más allá, como obligaciones deontológicas propias de las profesiones reguladas.

Además, en este sentido, hay que mencionar el artículo 16 Directiva 95/46/CE relativo a la confidencialidad del tratamiento, que establece que "las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido éste último, sólo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal". Esta última referencia al imperativo legal conduce, por tanto, a dos posibles fuentes de legitimación para que el encargado y el personal (al servicio de encargado y responsable) puedan tratar datos personales. Estas dos fuentes serían: el encargo realizado por el responsable y el imperativo legal.

Esta posibilidad debe entenderse como una vía de escape que permita al encargado (y también a las personas bajo la autoridad del responsable) desobedecer al responsable o, simplemente, poder actuar ante una falta de instrucciones, en virtud de una obligación legal imperativa. Cabría plantearse si, cuando el encargado del tratamiento acude al imperativo legal, como fuente de legitimación para realizar un determinado tratamiento ¿esto implica que se convierta en este momento en responsable del tratamiento? No debería tener esta implicación, ya que parece configurarse como una vía de escape y, por

tanto, no debería desvirtuar la naturaleza de encargado del tratamiento. Y es que el hecho de considerar que un encargado es responsable del tratamiento, cuando desobedezca al responsable, tiene una connotación negativa. No debería castigarse al encargado por actuar dentro de lo establecido en el artículo 16 Directiva 95/46/CE para obedecer un imperativo legal.

El GA29 menciona como criterio para identificar si estamos ante un responsable que el prestador de servicios deba contar con unos conocimientos especializados y, por tanto, el cliente responsable del tratamiento no tenga la capacidad para determinar los fines y los medios del tratamiento[279]. Sin embargo, de los ejemplos que expone el GA29 más bien se refiere a servicios que prestan colectivos que están fuertemente regulados y que deben atender a estas regulaciones, así como a su capacidad profesional. En estos servicios es fundamental la independencia frente a lo que pueda dictar el cliente. Esto implicará que sean los prestadores quienes deban decidir sobre el tratamiento de datos en virtud de estos conocimientos y de estas normativas.

El poder de control sobre el tratamiento provendrá de la naturaleza del servicio proporcionado. Pero en esta misma línea, puede suceder que un servicio que, en principio, puede exigir este tipo de conocimientos sea objeto de encargo por parte de un responsable del tratamiento que también tenga estos conocimientos y esté sujeto a estas regulaciones y que realice el encargo por distribuir simplemente la carga de trabajo. De esta forma, la situación puede ser extremadamente compleja de identificar[280].

[279] El GA29 cita como ejemplo el de los abogados (aunque en la versión en español indica "representantes procesales" lo que podría parecer que se refiere a los procuradores, en la versión en inglés se refiere a los *barrister* que se traduce como abogados). Los abogados utilizan la información que les proporcionan sus clientes en virtud de un mandato de estos. Sin embargo, esta actividad cuenta tradicionalmente con una base jurídica y además entiendo que a lo que apunta el GA29 es que los conocimientos que tienen estos profesionales implican una independencia frente a los dictados del cliente. Es decir, un abogado debe asesorar a su cliente de forma independiente y este cliente tiene una capacidad limitada de dar instrucciones. Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.*, pág. 32.

[280] En el ejemplo de los abogados, puede ser que un abogado encargue a otro parte de la gestión. En este caso, habrá que tener en cuenta la naturaleza de las tareas encomendadas y el poder de control de uno y otro para poder calificar el supuesto. Otro ejemplo que indica el GA29 es el de los asesores contables. Así, un asesor contable puede ser considerado responsable del tratamiento si recibe de su cliente instrucciones muy genéricas que le dejarán todo el poder de decisión. Sin embargo, podrá ser calificado como encargado del tratamiento si quien le contrata es una empresa con departamento contable plenamente capacitado para dar instrucciones concretas al asesor y que, por tanto, tiene esa capacidad de controlar el tratamiento de datos. *Ibídem*, pág. 33.

Otro criterio que apunta el GA29 es que en ciertas situaciones donde la complejidad de las operaciones de tratamiento sea importante, puede ser necesario dar un margen de maniobra más amplio a quienes realizan el tratamiento de datos. Incluso en estos casos sugiere el GA29 que puede ser necesaria una aclaración legal[281].

c. La relación contractual y la influencia de hecho

Además de poder acudir a la legislación o a la práctica jurídica, al igual que se indicaba respecto al responsable, también se ha de analizar si el poder de determinación emana de la capacidad de influencia de hecho. Cuando debemos diferenciar entre responsable y encargado, adquiere especial relevancia el análisis de la relación contractual, ya que, en estos casos, el encargo debe regularse por un contrato u otro acto jurídico (art. 17 Directiva 95/46/CE). Este contrato debe incluir un contenido específico: que el encargado sólo actúa conforme a las instrucciones del responsable y que las obligaciones relativas a las medidas de seguridad incumben también a este encargado. Se exige que el contrato conste por escrito o en forma equivalente.

El GA29 interpreta que este contrato no es decisivo ni constitutivo[282]. De nuevo se puede aplicar lo indicado para el responsable, de forma que debería darse mayor prevalencia a la realidad que a lo que se establezca en los contratos, si bien, inicialmente serán un indicio valioso para determinar si estamos ante un responsable o un encargado.

Si el proveedor de servicios, que implican un tratamiento de datos por cuenta del cliente, es quien elabora el contrato, por ejemplo porque elabora modelos estándar para todos sus clientes, esto no se considera motivo para entender que el cliente no pueda calificarse de responsable del tratamiento. El GA29 entiende que el cliente debe ser responsable ya que ha decidido libremente contratar el servicio y las condiciones contractuales que lo regulan[283].

[281] Así el GA29 menciona como ejemplo los tratamientos con fines históricos, científicos y estadísticos, en los que una organización intermediaria se encargue de codificar los datos que le proporcionen responsables y transmitirlos a otros responsables. Esta tarea conlleva un especial riesgo para la protección de los datos, por lo que justifica que la legislación establezca que esta organización intermediaria sea responsable del tratamiento. *Ibídem.*
[282] *Ibídem*, pág. 30.
[283] *Ibídem* pág. 29. Ver Capítulo VIII.

El GA29, al igual que hizo en referencia al responsable, ofrece algunos criterios que se podrán utilizar para diferenciar entre responsable y encargado en atención a los hechos[284]. Así, menciona aquellos rasgos que muestren que un sujeto tiene poder de control y que ayudarán a identificarlo como responsable y que, en caso contrario, lo identificarán como encargado del tratamiento. Como criterios que mostrarán el poder de control, el GA29 indica el nivel de instrucciones que proporcione el responsable del tratamiento, que determinará el margen de maniobra que se deja al encargado. También mostrará el control el seguimiento por el responsable del tratamiento de la ejecución del servicio, de forma que una supervisión estricta, por parte de éste, indicará que el responsable sigue teniendo el control pleno sobre el tratamiento.

Por último, hacer mención del criterio relativo a la visibilidad o la imagen que se proporcione a los interesados sobre quién es el responsable, como ya se indicó cuando se analizaba el concepto de responsable.

3. EL CONCEPTO EN OTRAS NORMAS DE DERECHO COMUNITARIO DERIVADO

3.1. El Reglamento 45/2001 de protección en el marco de las instituciones comunitarias

A raíz de la previsión que se había incluido en el Tratado de Ámsterdam, en el artículo 286.1 del Tratado constitutivo de la Comunidad Europea, donde se establecía que a partir del 1 de enero de 1999, los actos comunitarios relativos a la protección de personas respecto al tratamiento de datos personales y a la libre circulación de dichos datos serían de aplicación a las instituciones y organismos comunitarios, se aprobó el Reglamento 45/2001 para la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (Reglamento 45/2001).

Como especifica la norma en sus considerandos, el reglamento se inspira en las normas ya existentes en el ámbito de la armonización de legislaciones nacionales y

[284] *Ibídem* págs. 31 a 34.

aplicación de políticas comunitarias, tanto respecto a los derechos de las personas, cuyos datos se tratan, como con relación a las obligaciones de los responsables del tratamiento[285]. Además, las instituciones y los organismos comunitarios deberán respetar el derecho nacional de los Estados miembros, adoptado en aplicación de la Directiva 95/46/CE. Esto significa que no pueden prohibir o limitar la libre circulación de datos personales entre los Estados y destinatarios sujetos a estos derechos nacionales, por lo que por encima de esta regulación, en estos casos, tendrá que estar la legislación nacional, pese a tratarse de un reglamento comunitario y, por tanto, de aplicación directa.

El objeto del reglamento consiste en la garantía de protección de los derechos y libertades fundamentales de las personas físicas, en particular su derecho a la intimidad, en lo que respecta al tratamiento de los datos personales (art. 1 Reglamento 45/2001). Esta garantía la deben procurar las instituciones y los organismos creados por los Tratados constitutivos o en virtud de los mismos. El reglamento crea una autoridad de control que supervisará la aplicación de sus disposiciones a todas las operaciones de tratamiento que realicen las instituciones y organismos comunitarios: el Supervisor Europeo de Protección de Datos.

Esta norma contiene una definición propia de responsable del tratamiento, que es:

> ”la institución, organismo, dirección general, unidad u otra entidad organizativa comunitaria que por sí sola o conjuntamente con otras determine los fines y los medios del tratamiento de datos personales; cuando los fines y los medios del tratamiento estén determinados por un acto comunitario concreto, el responsable del tratamiento o los criterios específicos aplicables a su nombramiento podrán determinarse en tal acto comunitario;” (art. 2.d) Reglamento 45/2001).

Hay que entender aplicables a esta definición los criterios que se han seguido en la definición de la Directiva 95/46/CE. Este concepto es una traslación de la definición de la Directiva 95/46/CE al ámbito de las instituciones comunitarias. Esta adaptación ha

[285] “Las disposiciones aplicables a las instituciones y organismos comunitarios deben corresponder a las previstas para la armonización de las legislaciones nacionales o la aplicación de otras políticas comunitarias, sobre todo en materia de asistencia mutua; no obstante, puede ser necesario hacer precisiones y establecer disposiciones complementarias para garantizar la protección en el caso del tratamiento de datos personales efectuado por las instituciones y los organismos comunitarios.” “Esta observación es aplicable tanto a los derechos de las personas cuyos datos se tratan como a las obligaciones de las instituciones y organismos comunitarios responsables del tratamiento, y a los poderes de que debe disponer la autoridad de control independiente encargada de velar por la correcta aplicación del presente Reglamento.” “Procede que los derechos otorgados a la persona interesada y el ejercicio de los mismos no afecten a las obligaciones impuestas al responsable del tratamiento.” Considerandos 20-22 Reglamento 45/2001.

implicado modificar el elemento subjetivo para acomodarlo a la tipología organizativa de la UE. También se ha cambiado el reenvío a la legislación aplicable que, en esta definición se especifica como el reenvío a "un acto comunitario concreto".

3.2. La Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas

Hay que mencionar la Directiva 2002/58/CE[286], que sustituyó a la Directiva 97/66/CE[287], ya que regula, en el ámbito de los servicios de comunicaciones electrónicas, el tratamiento de datos personales y la protección de la intimidad[288]. La Directiva 95/46/CE, al considerarse la norma general, será de aplicación subsidiaria[289]. En el ámbito de aplicación, además de protegerse los derechos de las personas físicas, también se protegen en esta norma los intereses legítimos de las personas jurídicas, ya que ambos colectivos pueden ser abonados de este tipo de servicios.

Al ser un complemento de la Directiva 95/46/CE, la Directiva 2002/58/CE remite a ella para las definiciones, por lo que debería aplicarse todo lo comentado con relación al concepto de responsable del tratamiento. A estas definiciones se añaden en su artículo 2 otras referidas al sector específico que regula. Si bien en la Directiva 97/66/CE se incluía en estas definiciones la noción de "servicio de telecomunicación", que delimitaba el

[286] Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), DO L 201 de 31.7.2002. Esta directiva fue modificada por la Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15.3.2006 (DO L 101 de 13.4.2006) y por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores (Texto pertinente a efectos del EEE), DO L 337 de 18.12.2009.

[287] Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, DO L 24 de 30.1.1998.

[288] Esta directiva incluye, en su título, una distinción clara entre el tratamiento de datos personales y la intimidad. Asimismo, se le ha dado la denominación común de Directiva sobre privacidad y las comunicaciones electrónicas. En la privacidad se entienden incluidos los derechos de protección de datos y de intimidad. No se alude al derecho de protección de datos porque en 1997, cuando se aprobó la Directiva no se había reconocido aún este derecho, de forma autónoma.

[289] Las disposiciones de esta Directiva especifican y completan la Directiva 95/46/CE (art. 1.2 Directiva 2002/58/CE). Asimismo, se establece que "En el sector de las comunicaciones electrónicas es de aplicación la Directiva 95/46/CE, en particular para todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales que no están cubiertas de forma específica por las disposiciones de la presente Directiva, incluidas las obligaciones del responsable del tratamiento de los datos y los derechos de las personas. La Directiva 95/46/CE se aplica a los servicios de comunicaciones electrónicas que no sean de carácter público." (Considerando 10 Directiva 2002/58/CE).

ámbito de aplicación, en la Directiva 2002/58/CE este concepto se elimina. Se opta por incluir una remisión a las definiciones de la norma sectorial que regula en el ámbito comunitario el sector de las comunicaciones electrónicas[290].

No puede hablarse de un supuesto que aplique el reenvío previsto en el concepto de responsable de la Directiva 95/46/CE a otras leyes que puedan establecer los fines y medios del tratamiento. En la Directiva 2002/58/CE no se ha determinado claramente quien se entiende que es responsable del tratamiento ni los criterios para su nombramiento[291].

Hay que mencionar que se ha considerado que esta Directiva 2002/58/CE representa un ejemplo de evolución de la normativa de protección de datos, que pondría el foco en la tecnología[292]. La determinación de los sujetos obligados, sin tener en cuenta el concepto de responsable del tratamiento, sería una característica de esta evolución. Otra característica sería el desbordamiento del concepto de datos personales que se amplía a otras categorías, como los datos de tráfico, que se orientan a los equipos terminales, más que a las personas.

Sin embargo, esta tendencia señalada no parece que se haya consolidado en otra normativa similar. Además, la definición de los sujetos obligados, sin determinar su papel de responsable o de encargado, no ha sido más eficaz[293]. Por otro lado, la remisión a las

[290] Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco), DO L 108 de 24.4.2002. Respecto a la definición de los sujetos obligados hay que mencionar las repetidas peticiones del GA29 en el marco de las reformas realizadas a la Directiva 2002/58/CE, precisamente con el fin de aclarar los conceptos y los cometidos específicos de los diferentes sujetos implicados en estos servicios. Así, se pide más claridad en las nociones de "red pública de comunicaciones" y "servicios de comunicaciones electrónicas", especialmente en el caso de redes híbridas públicas y privadas. Dictamen 8/2006 sobre la revisión del marco regulador de las redes y los servicios de comunicaciones electrónicas, con especial atención a la Directiva sobre la privacidad y las comunicaciones electrónicas, 01611/06/ES WP 126, 26.9.2006, Grupo de trabajo Artículo 29 sobre la protección de datos, pág. 7 y Dictamen 2/2008 sobre la revisión de la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas (Directiva sobre privacidad), 00989/08/ES WP 150, 15.5.2008, Grupo de trabajo Artículo 29 sobre la protección de datos, págs. 4 a 5.

[291] Hay que recordar lo mencionado anteriormente en referencia al Considerando 47 Directiva 95/46/CE.

[292] Y. POULLET, "Pour une troisième génération de réglementation de protection des données", M. VERÓNICA, P. PALAZZI (Coord.) VVAA, *Défis du droit à la protection de la vie privée. Challenges of privacy and data protection law*, Bruylant, Bruxelles, Belgique, 2008, págs. 52 a 54.

[293] Hay que recordar el asunto *Probst* mencionado. Sentencia del TJUE de 22 de noviembre de 2012 *Probst*, C-119/12, EU:C:2012:748.

definiciones de la Directiva 95/46/CE debería implicar que a estos sujetos obligados se les adjudicase uno de estos papeles, con el fin de completar la regulación.

3.3. La Decisión marco 2008/977/JAI relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal

La estructura en pilares, anterior a la aprobación del Tratado de Lisboa, requirió de la aprobación de la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (Decisión Marco 2008/977/JAI)[294]. La cooperación policial y judicial en materia penal se incluía en el tercer pilar y, en consecuencia, se había excluido del ámbito de aplicación de la Directiva 95/46/CE, norma que sólo regulaba la materia incluida en el primer pilar, el comunitario.

La división en pilares había originado diversos instrumentos jurídicos y, por eso, se adoptó, en este caso, una decisión marco cuyos efectos son similares a los de una directiva[295]. El objeto de la decisión marco era el intercambio de datos en el marco de la cooperación policial y judicial entre las autoridades competentes en la materia[296]. Por tanto, se delimitaba el ámbito de aplicación al tratamiento de datos transmitidos o puestos a disposición entre Estados miembros (art. 1 Decisión marco 2008/977/JAI), lo que implicaba que no se aplicaba a la recopilación y tratamiento de datos personales en el ámbito nacional[297].

---

[294] Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, DO L 350 de 30.12.2008.

[295] Las decisiones marco se introdujeron mediante la modificación del Tratado de la Unión Europea por el Tratado de Amsterdam (art. 32.2.b) TUE). Estas decisiones las adoptaba el Consejo el ámbito del Título VI TUE con el objetivo de aproximar la legislación de los Estado miembros. Por tanto, al igual que sucede con las directivas, las decisiones marco obligaban a los Estados miembro en cuanto al resultado que debía obtenerse pero dejaba a las autoridades nacionales la elección de la forma y de los medios. Estas decisiones no tenían efecto directo. El Tratado de Lisboa ha eliminado la estructura de pilares y, como consecuencia ha uniformizado también los procedimientos legislativos, de forma que también ha desparecido la utilización de los instrumentos jurídicos específicos que se crearon para los pilares, como las decisiones marco.

[296] Por tanto, esta decisión marco se refiere a la materia incluida en el tercer pilar mencionado.

[297] GUASCH PORTAS critica esta limitación en el ámbito de aplicación de la Decisión marco 2008/977/JAI al tratamiento transfronterizo de datos y resalta que, en ocasiones, será difícil determinar cuándo es tratamiento transfronterizo y, por tanto, incluido en el ámbito de aplicación de la decisión o tratamiento nacional de datos que quedaría fuera de su ámbito de aplicación. V. GUASCH PORTAS, *Las transferencias internacionales de datos en la normativa española y comunitaria*, Agencia Española de Protección de Datos, BOE, Madrid, 2014, pág. 291.

La Decisión marco contiene también una definición de responsable del tratamiento que sólo difiere de la contenida en la Directiva 95/46/CE en la supresión del reenvío al derecho nacional o comunitario para la determinación del mismo (art. 2.i) Decisión marco 2008/977/JAI). Sin embargo, quiero destacar que, aunque se incluya la definición de responsable, en la regulación sólo se menciona en los artículos 17, 18, 19 y 25 Decisión marco 2008/977/JAI. Estas menciones se realizan principalmente en referencia a la obligación del responsable del tratamiento de atender los derechos del interesado de acceso, rectificación, supresión o bloqueo (art. 17 y 18 Decisión marco 2008/977/JAI) y también al derecho de reparación que tienen estos interesados (art. 19 Decisión marco 2008/977/JAI).

La falta de mención del responsable respecto a otras obligaciones es resultado de la falta de asignación de las mismas de forma expresa, lo que, como se verá, cuando se aborde el estatuto del responsable, es algo habitual. Sin embargo, en este caso, otra razón es que se incluye otro sujeto obligado: la autoridad competente. Este sujeto también se define en la decisión[298].

Esta dualidad en el sujeto obligado es confusa, ya que supone un solapamiento y plantea la pregunta de si deben coincidir o no. Es decir, cuando se menciona a la autoridad competente como sujeto obligado a cumplir una de las obligaciones de la decisión marco, ¿debe aplicarse también la definición de responsable del tratamiento? O basta que cumpla con el criterio de la definición de autoridad competente. En ese caso, habría algunas obligaciones que debería cumplir aquel sujeto que responda a los requisitos de la definición de autoridad competente y habría otras obligaciones (las mencionadas) que debería cumplir el sujeto que responda a los requisitos de la definición de responsable del tratamiento. No parece ser ésta la respuesta, sino que debe entenderse que ambas definiciones deben complementarse y el sujeto obligado deberá ser responsable del tratamiento y autoridad competente.

[298] "Autoridades competentes, los servicios u organismos creados en virtud de actos jurídicos adoptados por el Consejo al amparo del título VI del Tratado de la Unión Europea, así como las autoridades policiales, judiciales, aduaneras y otras autoridades competentes de los Estados miembros autorizadas por el Derecho nacional a tratar datos personales en el ámbito de la presente Decisión Marco" (art. 2.h) Decisión marco 2008/977/JAI).

Este defecto se ha corregido en la Propuesta de directiva policía presentada por la Comisión Europea para sustituir a la Decisión marco 2008/977/JAI, en su versión aprobada por el Parlamento Europeo en primera lectura[299]. De esta forma, en la definición de responsable del tratamiento se ha definido el elemento subjetivo como "la autoridad pública competente[300]. También se ha vuelto a introducir el reenvío a la legislación nacional o de la Unión Europea para determinar al responsable.

4. UNA NECESARIA REFERENCIA A LA CARTA DE DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA

Tras el fracaso obtenido en el proceso de ratificación del Tratado constitucional de la Unión Europea con el rechazo manifestado por parte de los ciudadanos en los referéndums que se llevaron a cabo en Francia y Países Bajos, se elaboró el Tratado de Lisboa que reformaba los tratados y que se firmó el 13 de diciembre de 2007, entrando en vigor el 1 de diciembre de 2009. Este Tratado conlleva importantes modificaciones en materia de derechos fundamentales, modifica la estructura de pilares y, además, establece que la Carta de derechos fundamentales de la Unión Europea (Carta UE)[301] sea un texto jurídicamente vinculante (art. 6.1 TFUE)[302].

---

[299] Al igual que sucede con la Directiva 95/46/CE, la Decisión marco 2008/977/JAI es objeto del proceso de reforma que se lleva a cabo en el ámbito de la Unión Europea respecto al marco regulador de la protección de datos. Al desaparecer la estructura en pilares y los instrumentos jurídicos que, como la decisión marco, habían surgido para regular en función de esta estructura, se ha optado por elegir la forma de una directiva que sustituirá la actual decisión y que además ampliará su ámbito de aplicación. De esta forma la futura directiva no sólo se referirá a los intercambios de datos entre Estados miembros, sino que se aplicará en general a los tratamientos de datos realizados por las autoridades competentes con fines de prevención, investigación, detección y enjuiciamiento de infracciones penales o de ejecución de sanciones penales y las condiciones para la libre circulación de dichos datos personales (art. 1.1 PCE-Directiva Policía).

[300] Así la definición es "«responsable del tratamiento»: la autoridad pública competente que sola o conjuntamente con otras determine los fines y medios del tratamiento de datos personales; en caso de que los fines y medios del tratamiento estén determinados por el Derecho de la Unión o la legislación de los Estados miembros, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho de la Unión o por la legislación de los Estados miembros;" y se complementa con la definición de "«autoridades competentes»: toda autoridad pública competente para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales;" (art. 3, apartados 6 y 14 Propuesta CE Directiva Policía). Durante el trámite parlamentario únicamente se eliminó el término "condiciones" que se añadió a los aspectos sobre los que el responsable tenía poder de determinación: los fines y medios del tratamiento de datos.

[301] Carta de los Derechos Fundamentales de la Unión Europea, DO C 83 de 30.3.2010 (versión consolidada).

[302] El artículo 6 del TUE establece: "1. La Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados. Las disposiciones de la Carta no ampliarán en modo alguno las competencias de la Unión tal como se definen en los Tratados. Los derechos, libertades y principios enunciados en la Carta se interpretarán con arreglo a las disposiciones generales del título VII de la Carta por las que rige su

La Carta UE supone por primera vez tener un catálogo de derechos propio de la Unión Europea, lo que permite que el TJUE pueda acudir al mismo, en vez de tener que construir un catálogo a golpe de sentencia y remitirse a tratados internacionales como el CEDH y a las tradiciones constitucionales comunes de los Estados miembros.

La Carta UE ya había sido aceptada por las instituciones europeas (Parlamento Europeo, Comisión y Consejo) mediante acuerdo interinstitucional, el 7 de diciembre de 2000[303]. Pese a no ser un texto vinculante jurídicamente, fuera de este contexto interinstitucional, tuvo enseguida una gran repercusión y empezó a utilizarse como referencia por el TJUE y por los tribunales nacionales[304]. Hay que destacar el caso de España, donde el Tribunal Constitucional, precisamente en su importantísima STC 292/2000, de 30 de noviembre, relativa al reconocimiento del derecho a la protección de datos, como un derecho autónomo, se fundamentó en la Carta UE. Y es que la Carta UE incluyó en su artículo 8, como derecho autónomo, el derecho a la protección de datos:

> "Artículo 8. Protección de datos de carácter personal. 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto a estas normas estará sujeto al control de una autoridad independiente" (art. 8 Carta UE).

Este derecho se diferenciaba claramente del derecho a la vida privada que se incluía en el artículo 7 Carta UE, derecho que había servido de base jurídica hasta ese momento para extraer la protección de los datos personales, en el ámbito del CEDH[305].

---

interpretación y aplicación y teniendo debidamente en cuenta las explicaciones a que se hace referencia en la Carta, que indican las fuentes de dichas disposiciones. 2. La Unión se adherirá al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Esta adhesión no modificará las competencias de la Unión que se definen en los Tratados. 3. Los derechos fundamentales que garantiza el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y los que son fruto de las tradiciones constitucionales comunes a los Estados miembros formarán parte del Derecho de la Unión como principios generales."

[303] Acuerdo atípico publicado en el DO C de 18.12.2000.

[304] Como indica ALONSO GARCÍA, la Carta se comenzó a utilizar como referencia por los Abogados Generales del Tribunal de Justicia y por el Tribunal de Primera Instancia, aunque no fue hasta junio de 2006 en el asunto Parlamento Europeo v. Consejo en el que la invocó expresamente. R. ALONSO GARCÍA, *Sistema jurídico de la Unión Europea*, 2ª ed., Aranzadi, Cizur Menor (Navarra), 2010, pág. 298.

[305] "Artículo 7. Respeto de la vida privada y familiar. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.", Carta UE.

La Carta UE fue puesta al día el 12 de diciembre de 2007, en el marco de la reforma que dio lugar al Tratado de Lisboa y los Presidentes del Parlamento, del Consejo y de la Comisión Europea la firmaron y la volvieron a proclamar solemnemente.

Los sujetos obligados a respetar este catálogo serán las instituciones, órganos y organismos de la UE[306]. Las instituciones son el Parlamento Europeo, el Consejo, el Consejo Europeo, la Comisión Europea, el Tribunal de Justicia de la Unión Europea, el Banco Central Europeo y el Tribunal de Cuentas[307]. Los órganos y organismos serán todos los creados por los tratados y por el derecho derivado.

También son sujetos obligados los Estados miembros, cuando apliquen el derecho de la Unión, por lo que podrán regular con autonomía, al margen del derecho comunitario, los derechos incluidos en el catálogo de la Carta UE[308]. Además se especifica en las explicaciones a la Carta UE que se aplicará, tanto a las autoridades centrales, como a las instancias regionales o locales, así como a los organismos públicos cuando aplican el Derecho de la Unión.

Con relación a la eficacia de la Carta UE frente a terceros particulares, el TJUE ha reconocido la eficacia horizontal siempre que se trate de relaciones jurídicas en las que se aplique el derecho de la Unión. Esto sucederá en el caso de particulares que realicen algún tratamiento de datos personales que quede incluido en el ámbito de aplicación de las Directivas que regulan estos tratamientos[309].

[306] El ámbito de aplicación se establece en el artículo 51 Carta UE.
[307] Artículo 13 TUE.
[308] No debe entenderse exclusivamente a la aplicación en sentido estricto del derecho de la Unión, entendida como ejecución, sino también cuando pretendan derogar o excepcionar el derecho. Esta es la llamada doctrina de la incorporación. M. ARENAS RAMIRO. *El derecho fundamental a la protección de datos personales en Europa, op. cit.*, pág. 255, R. ALONSO GARCÍA, *Sistema jurídico de la Unión Europea*, *op. cit.* pág. 320. La Comisión Europea indicaba que "la Carta no se aplica en las situaciones de violaciones de los derechos fundamentales que no guarden ninguna relación con el Derecho de la Unión. Los Estados miembros tienen su propio sistema de protección de los derechos fundamentales, mediante los órganos jurisdiccionales nacionales, y la Carta no los sustituye. Corresponde, por tanto, a las jurisdicciones nacionales, garantizar el respeto de los derechos fundamentales y a los Estados miembros adoptar las medidas necesarias de acuerdo con su legislación nacional y sus obligaciones internacionales. En tales situaciones, la Comisión no dispone de poderes para intervenir como guardiana de los Tratados." Comunicación de la Comisión Europea sobre la estrategia para la aplicación efectiva de la Carta de los Derechos Fundamentales por la Unión Europea, COM(2010) 573 final, Bruselas, 19.10.2010, pág. 11.
[309] Por tanto, la Directiva 95/46/CE y la Directiva 2002/58/CE. M. ARENAS RAMIRO. *El derecho fundamental a la protección de datos personales en Europa, op. cit.*, pág. 256.

Además, hay que tener en cuenta que el ámbito de aplicación de la Carta UE es más amplio que el de la Directiva 95/46/CE, ya que el Tratado de Lisboa eliminó la estructura de pilares. De esta forma, la Carta UE también engloba la esfera de la cooperación policial y judicial en materia penal que antes conformaba el tercer pilar. La jurisdicción del TJUE también se extiende a las materias propias de esta esfera de cooperación policial y judicial en materia penal. En cuanto a la política exterior y de seguridad común, el antiguo segundo pilar, el nuevo Tratado lo mantiene diferenciado. Sin embargo, se prevé una extensión importante de la jurisdicción del TJUE en este ámbito. Se reconoce así una vía jurisdiccional que permitiría a los particulares plantear la eventual vulneración de sus derechos fundamentales por una medida adoptada por el Consejo en este ámbito[310].

Por último, indicar que el Tratado de Lisboa introdujo el artículo 16 TFUE, que en su apartado 2 introduce una base jurídica específica para la adopción de normas relativas a esta materia de protección de datos, base que se utiliza actualmente para la tramitación de la reforma de la Directiva 95/46/CE[311].

[310] El artículo 275 del TFUE prevé la competencia del tribunal para entender de los recursos de anulación que se planteen contra las decisiones adoptadas por el Consejo en el ámbito de la política exterior y de seguridad común que establezcan medidas restrictivas frente a personas físicas o jurídicas. M. DÍAZ CREGO, *Protección de los derechos fundamentales en la Unión Europea y en los Estados miembros*, Reus, Madrid, 2009, pág. 180.
[311] Ver Capítulo IX.

CAPÍTULO III

LA RECEPCIÓN DEL CONCEPTO DE RESPONSABLE EN LAS LEGISLACIONES EUROPEAS NACIONALES DE PROTECCIÓN DE DATOS

Tras el análisis del concepto de responsable en la Directiva 95/46/CE y en los instrumentos internacionales relativos al derecho a la protección de datos, procede realizar una aproximación al concepto en las legislaciones nacionales europeas. De esta forma, se analizarán especialmente las divergencias existentes entre la regulación de la Directiva 95/46/CE y la transposición que han realizado las leyes nacionales del concepto. El análisis se detendrá en la legislación española, en el que se incluirán las características específicas del concepto.

1. LA RECEPCIÓN DEL CONCEPTO DE RESPONSABLE EN LAS LEGISLACIONES EUROPEAS NACIONALES DE PROTECCIÓN DE DATOS: ANÁLISIS COMPARATIVO

¿Cómo se ha transpuesto el concepto de responsable de la Directiva 95/46/CE en las legislaciones europeas nacionales? ¿Se respeta su naturaleza de concepto autónomo del derecho europeo? Para responder a esta pregunta se han examinado las leyes de los países miembros de la Unión Europea y los países de la Asociación Europea de Libre Comercio (AELC), Noruega, Islandia y Liechtenstein (es decir, todos los que forman parte de la AELC, excepto Suiza) a los que también se aplica la Directiva 95/46/CE[312].

El análisis del concepto de responsable se realizará con la metodología utilizada en el anterior capítulo y, por tanto, se abordarán los diferentes elementos subjetivo, objetivo y funcional[313]. El texto de los diversos conceptos que se analizan a continuación se incluye en Anexo I[314].

[312] La aplicación de la Directiva 95/46/CE es fruto del Acuerdo del Espacio Económico Europeo (EEE), Decisión del Comité Mixto del EEE nº 83/1999, de 25 de junio de 1999, por la que se modifica el Protocolo 37 y el anexo XI (Servicios de telecomunicaciones) del Acuerdo EEE, DO L 296 de 23.11.2000.

[313] Debe tenerse en cuenta que se ha realizado un estudio de las leyes que principalmente regulan la materia del derecho a la protección de datos en los países objeto del estudio, sin incluir normas adicionales que pueden regular esta materia ni otras disposiciones que pudieran afectar a la misma. Las leyes que se han examinado se incluyen en el apartado dedicado a la Documentación.

[314] Se omitirán, por tanto, las referencias a los preceptos de las leyes que contienen estos conceptos.

1.1. El elemento subjetivo

Hay que recordar que este primer elemento se refería al tipo de sujeto que puede considerarse responsable y que en la Directiva 95/46/CE se definía como: "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo" (art. 2.d) Directiva 95/46/CE).

Las leyes europeas analizadas contienen algunas divergencias en sus conceptos respecto a este elemento. La mayoría de estas diferencias responde a la necesaria adaptación del elemento a los ordenamientos jurídicos nacionales. Esto es especialmente importante en aquellas normas en las que se establece una delimitación de los sujetos que se entenderían dentro del sector público y del sector privado. Principalmente, esto se produce en las leyes que incluyen una regulación diferenciada para ambos sectores, como sucede en las Leyes italiana, alemana o en la española, ya que es imprescindible que quede claro a qué sujetos debe aplicarse una u otra regulación[315].

En algunas leyes se ha simplificado el elemento subjetivo respecto a la Directiva 95/46/CE[316]. Sin embargo, estas simplificaciones, en ocasiones responden a una técnica jurídica en la que el elemento se completa con otras definiciones[317] o con otras disposiciones de la ley[318], lo que no parece lo más acertado si se busca seguridad jurídica, especialmente en los supuestos en los que la remisión no se realiza expresamente desde la

[315] En la Ley alemana se incluye una regulación pormenorizada de lo que se considera entidad pública o privada, con referencia específica a la estructura en *Länder*. No hay que olvidar que la separación en la regulación entre sector público y privado que contenía ya la Ley federal alemana de 1990 originó que, en la primera propuesta de la Directiva 95/46/CE, se incluyera esta separación entre ambas regulaciones que no se mantuvo en el texto final.

[316] Las Leyes irlandesa, sueca, noruega, maltesa e inglesa aluden simplemente a una "persona". En el caso de la Ley inglesa, como aclara la autoridad de control inglesa debe ser una persona reconocida por la ley como tal, un individuo, organizaciones y otras entidades mercantiles o no: "*22 A data controller must be a "person" recognised in law, that is to say: individuals; organisations; and other corporate and unincorporated bodies of persons." The guide to data protection*, *Information Commissioner's Office* (ICO), pág. 26. http://www.ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Practical_application/the_guide_to_data_protection.pdf, (fecha consulta: 24.8.13).

[317] Así sucede en las Leyes chipriota, alemana y eslovena.

[318] Por ejemplo, la Ley polaca recoge como elemento subjetivo de la definición: el órgano, unidad organizativa, establecimiento o persona al que se refiere al artículo 3. El artículo 3 Ley polaca establece el ámbito de aplicación de la ley y enumera los sujetos obligados, de forma que especifica que se podrá aplicar la ley, entre otros, a unidades organizativas estatales y municipales y unidades organizativas que no tengan personalidad jurídica, si realizan alguna parte del tratamiento como parte de su negocio o actividad profesional o para llevar a cabo algún objetivo establecido legalmente. Todas estas entidades deben además estar ubicadas en el territorio de la República de Polonia o en un tercer país, si se utilizan en el tratamiento de datos medios técnicos ubicados en el territorio polaco.

definición de responsable, sino que el desglose de los sujetos obligados se realiza en otro precepto[319].

De esta forma, por un lado, tendríamos la definición de responsable con un elemento subjetivo simplificado y, por otro lado, tendríamos un desglose detallado de los sujetos obligados, pero que estaría en otra disposición, por ejemplo, relativa al ámbito de aplicación. Esto puede implicar que no todos los sujetos obligados tendrán que revestir la calidad de responsable (pueden ser, por ejemplo, encargados del tratamiento) y el desglose sólo puede tomarse, como una pauta de los sujetos que podrían calificarse como tales. Esta manera de exponer el elemento subjetivo no tiene tanta consistencia como si se integrara en el concepto.

Se ha constatado que hay leyes que han ido más allá de lo previsto por la Directiva 95/46/CE. En este sentido, varias leyes han contemplado expresamente la posibilidad de que el sujeto que puede ser responsable carezca de personalidad jurídica[320]. La Ley italiana ha especificado expresamente que la responsabilidad debe recaer sobre la empresa y no sobre el empleado, tal como defiende el GA29[321]. Por el contrario, la Ley irlandesa ha establecido la designación formal de funcionarios en el ámbito del sector público, como responsables, lo que iría en contra de la tendencia generalizada apuntada[322].

---

[319] La Ley croata establece como elemento subjetivo "una persona física o jurídica, estado u otro órgano" que debe completarse con lo que establece el artículo 3 Ley croata que indica que la ley se aplica a los tratamientos de datos personales que llevan a cabo órganos del estado, órganos autónomos locales y regionales y personas físicas y jurídicas, las oficinas de representación y las oficinas de filiales de personas jurídicas extranjeras y los representantes de las personas físicas y jurídicas extranjeras. La Ley checa alude a "cualquier entidad" (*any entity*) pero este elemento se puede entender completado en el artículo 3.1 Ley checa, que establece los sujetos a los que se aplicará la ley y que los describe como: autoridades estatales, órganos territoriales autónomos, otros órganos de la autoridad pública y personas físicas y jurídicas.

[320] Así sucede en la legislación española y también en las Leyes chipriota, húngara y polaca. Asimismo, otras leyes que no incluyen expresamente esta inclusión de sujetos que no tienen personalidad jurídica, en sus definiciones hacen referencia a entidades como departamentos o unidades (Ley italiana), oficinas de órganos (Ley austríaca) o asociaciones de hecho (Ley belga) que parecen apuntar en esta dirección.

[321] En este sentido, la Ley italiana especifica que el responsable será la entidad como un todo o el departamento o unidad que tenga poder de decisión autónomo (art. 28 Ley italiana).

[322] De esta forma, cuando una autoridad respecto a parte o a la totalidad de datos personales que mantiene, designe un funcionario como responsable del tratamiento o encargado del tratamiento, mientras esta designación esté en vigor, este funcionario será considerado, con respecto a lo establecido en la ley irlandesa, como responsable del tratamiento o como encargado del tratamiento y la ley, por tanto, no se aplicará a la autoridad, con relación a los datos concernidos sino a este funcionario (art. 1.3.a Ley irlandesa). Como consecuencia de la aplicación de esta regla se establece que, en caso de que se realice esta designación de un funcionario como responsable o encargado, el resto de funcionarios que trabajen para la autoridad designante serán considerados a los efectos de la aplicación de la ley irlandesa, como empleados del funcionario designado (art. 1.3.c) Ley irlandesa). Además se regula de forma específica esta designación

1.2. El elemento objetivo

El objeto material sobre el que actúa el responsable es el elemento objetivo que en la Directiva 95/46/CE es "el tratamiento de datos personales" (art. 2.d) Directiva 95/46/CE). La mayoría de las leyes europeas ha escogido el mismo[323]. Sin embargo, pese a esta apariencia de similitud, al analizar las definiciones de lo que las leyes consideran tratamiento de datos personales e, incluso, de lo que son datos personales, se observan diferencias en la enumeración de las operaciones que conforman el tratamiento[324]. No obstante, estas diferencias no son relevantes, ya que la enumeración que realizaba la directiva no era exhaustiva y, por tanto, dejaba margen de maniobra a los Estados miembros, para que amoldaran la lista a sus necesidades.

Hay que resaltar también, con relación al tratamiento de datos, que algunas leyes inciden en algunas de las operaciones incluidas en esta noción, de forma que incluso se han elaborado definiciones de las mismas[325]. Estas operaciones sobre las que las leyes han

---

en caso del Ministerio de Defensa y de la *Garda Síochána*. En caso del Ministerio de Defensa y respecto a los datos relativos a las fuerzas de defensa, se establece que el responsable deberá ser un oficial de la Fuerza de Defensa Permanente (art. 1.3.b Ley irlandesa). En la Ley inglesa se encuentra un supuesto específico, similar al indicado en la Ley irlandesa de designación formal del responsable. Esto sucede con la determinación del responsable en el Reino Unido que se refiere a la Corona y el Parlamento. Así, por ejemplo, cuando los fines y la manera en que los datos se tratan los determine cualquier persona que actúe por cuenta de la *Royal Household* (Casa Real), el responsable del tratamiento será el *Keeper of the Privy Purse* (el Encargado de los Gastos Personales) (Sección 63 Ley inglesa) o respecto a la *House of Commons* (Casa de los Comunes) o de la *House of Lords* (Casa de los Lores) el responsable será el *Corporate Officer* (Oficial Corporativo) de la respectiva Casa (Sección 63A Ley inglesa).

[323] Las leyes que respetan el contenido de la Directiva 95/46/CE y aluden al tratamiento de los datos son las de: Bélgica, Bulgaria, Chipre, Croacia, Dinamarca, Estonia, Eslovaquia, Eslovenia, España, Francia, Grecia, Países Bajos, Hungría, Letonia, Lituania, Luxemburgo, Malta, Polonia, Portugal, Reino Unido, República Checa, Rumanía, Suecia, Islandia y Noruega.

[324] De esta forma, se concluye que hay diferencias en las leyes de Bulgaria, Chipre, Croacia, Eslovenia, Eslovaquia, Grecia, Países Bajos, Hungría, Italia, Lituania, Polonia, Reino Unido, República Checa, Islandia y Noruega.

[325] En la Ley griega se incluye la definición de "interconexión" (*interconection*) (art. 2.f) Ley griega). También se incluye una definición de interconexión, similar al de la Ley griega, en la Ley portuguesa (art. 3.i) Ley portuguesa). En la Ley Países Bajos se definen algunas operaciones incluidas en la definición de tratamiento, como la de recogida de datos o la provisión de datos (art. 1, apartados n) y o) Ley Países Bajos). También la Ley italiana introduce las definiciones de las operaciones de comunicación (*comunicazione*), diseminación (*diffusione*) y bloqueo (*blocco*) (art. 4.1 apartados l), m) y o) Ley italiana). En la ley lituana se añade un concepto relativo a la comunicación de datos debido a que se contiene en esta norma una regulación específica respecto a esta operación (art. 2.3 Ley lituana). La Ley polaca define la operación de supresión (art. 7.3 Ley polaca). En la Ley checa se incluyen definiciones de la recogida de datos, la conservación de los datos, el bloqueo y la liquidación de los datos (art. 4.f Ley checa). En la Ley rumana se incluye una definición del almacenamiento (*storage*) (art. 3.c) Ley rumana). La Ley sueca incluye una definición de lo que se entiende como bloqueo (Sección 3 Ley sueca) y la Ley eslovaca

querido reforzar su regulación son aquellas sobre las que se prevé un mayor riesgo para los datos: las que se refieren al momento de la recogida de datos, la comunicación de datos y a la fase de finalización del tratamiento.

Otro grupo de leyes han establecido como elemento objetivo el dato personal, el objeto último sobre el que recae la acción del responsable. Hay que destacar la Ley alemana, cuya definición de responsable incluye importantes diferencias respecto a la de la directiva. En esta ley, el elemento funcional, en vez de una capacidad de control, contempla principalmente unas capacidades ejecutivas del responsable, de forma que el control sólo se refleja en la posibilidad que tiene el responsable de encargar a un tercero el tratamiento. El elemento objetivo es el dato, ya que estas capacidades ejecutivas son las operaciones que se realizan sobre el mismo[326].

Algunas leyes han establecido que debe atenderse a otras informaciones que posea o pueda poseer el responsable para determinar si estamos ante datos personales. Y es que estas normas diferencian entre los datos recogidos del interesado y los que producen los responsables durante el tratamiento[327]. Asimismo, en otras leyes, para considerar si se puede entender que hay datos personales, se atiende a los medios técnicos a los que pueda acceder el responsable para poder identificar al interesado[328]. Este último criterio sería

---

contiene definiciones de operaciones relativas a la comunicación de datos, destrucción y bloqueo de datos (Sección 4.3.a, apdos 1 a 6 Ley eslovaca).

[326] Los otros supuestos que han optado por estimar que el elemento objetivo es el dato personal son las Leyes austríaca e irlandesa.

[327] La Ley irlandesa en la definición de tratamiento se refiere a dos tipos de información (información o datos) sobre los que pueden realizarse las operaciones enumeradas (art. 1.1 Ley irlandesa). Para valorar si la persona puede ser identificada o no, se está a los datos, y también a lo que se denomina información que posea o pueda poseer el responsable. En la Ley inglesa, en la definición de *"personal data"* (art. 1.1 Ley inglesa) también se especifica que deben tenerse en cuenta, en la identificación del interesado, los datos y otra información que esté en posesión o que pueda estar en posesión del responsable del tratamiento. Esta información incluye las opiniones sobre el individuo y cualquier indicación de las intenciones del responsable del tratamiento o de otra persona respecto a este individuo. Como se puede observar, lo que hace la ley inglesa es aclarar que deben analizarse, no sólo los datos que se obtengan del interesado, sino que también se debe tener en cuenta toda la información que maneje el responsable y la que elabore, fruto del tratamiento, y pueda asignarse al individuo.

[328] La Ley francesa (art. 2 Ley francesa) y la Ley húngara (Sección 4.3 Ley húngara) aluden a los medios de que disponga el responsable para poder identificar al interesado. De esta forma, ya no se centra la regulación en otras informaciones que tenga el responsable, sino en sus capacidades técnicas o materiales para poder gestionar la información y llegar a la identificación del interesado. Por último, en la misma definición de datos de la Ley austríaca, se establece otra definición relativa a los "datos indirectamente personales". Estos datos se definen como aquellos que para un responsable, un encargado del tratamiento o el destinatario de una transmisión, se refieran a un individuo, de forma que el responsable, encargado del tratamiento o destinatario de una transmisión no puedan establecer la identidad del interesado de una forma legal (parágrafo 4.1 Ley austríaca). Por tanto, habrá que estar a lo que se interpreta como "forma legal". Es

resultado de acoger la orientación que proporciona la directiva, que para determinar si una persona es identificable, estima que hay que considerar los medios que puedan ser razonablemente utilizados por el responsable o por cualquier otra persona, para identificar a esa persona (Considerando 26 Directiva 95/46/CE).

Resulta llamativo que aún queden leyes que contemplan en su elemento objetivo al fichero, reducto del pasado de una informática centrada en la capacidad de almacenamiento, más que en la interconexión y la interacción[329].

1.3. El elemento funcional

Un tercio de las leyes europeas conserva el elemento funcional sin cambios respecto al que establece la Directiva 95/46/CE: la capacidad del responsable de determinar los fines y los medios del tratamiento[330]. En las otras leyes hay cambios en la capacidad y también en los aspectos en los que se refleja esta capacidad.

1.3.1. La capacidad de determinar del responsable

Respecto a los cambios en la capacidad de determinar, la mayoría de leyes que han optado por modificarla se refieren a la capacidad de "decidir", bastante similar en su significado a determinar[331]. No obstante, también hay otras leyes que han elegido los términos "controlar" y "establecer"[332].

---

importante esta categoría de datos, ya que permiten excluir el cumplimiento de gran parte de las obligaciones que establece la ley.

[329] Estas son las Leyes finlandesa y de Liechtenstein.

[330] El elemento funcional se mantiene sin cambios respecto al que establece la Directiva 95/46/CE en las Leyes de Chipre, Croacia, Dinamarca, Eslovenia, Países Bajos, Hungría, Letonia, Lituania, Luxemburgo, Portugal y Noruega. Si bien, hay que matizar el caso de la Ley húngara que en un principio incluye lo mismo que la Directiva 95/46/CE al indicar que "determina los fines y medios del tratamiento de datos". Sin embargo añade después: "realiza y ejecuta decisiones concernientes al tratamiento de datos (incluyendo los medios utilizados) o contrata un encargado del tratamiento para ejecutarlo". Por tanto, a la capacidad de determinar fines y medios del tratamiento se añade la de realizar y ejecutar decisiones respecto a éste. Esta mención, sin embargo, aparece como contraposición a la posibilidad de que el responsable decida que estas capacidades de realizar y ejecutar decisiones las lleve a cabo el encargado del tratamiento, si decide contratar a este sujeto. Por tanto, lo que definiría al responsable sería la primera parte que es igual a la Directiva 95/46/CE.

[331] En el Diccionario de la lengua española, de la RAE, 22ª ed., se define "decidir" como "1. Cortar la dificultad, formar juicio definitivo sobre algo dudoso o contestable, 2. Resolver (tomar determinación de algo), 3. Mover a alguien la voluntad, a fin de que tome cierta determinación". El término "determinar" se define como "1. Fijar los términos de algo, 2. Distinguir, discernir, 3. Señalar, fijar algo para algún efecto, 4. Tomar resolución, 5. Hacer tomar una resolución". Se ha optado por la capacidad de decidir en las Leyes

Un caso singular lo constituye la Ley alemana que, como ya se ha mencionado, no incluye la capacidad de determinar, sino que alude a capacidades ejecutivas propias de un tratador (tratamiento, recogida y uso). Sin embargo, como el concepto menciona la posibilidad de que el responsable encargue este tratamiento a un tercero, en este poder de encargo es donde se refleja el poder de determinación. En este sentido, la Ley alemana ha mantenido algunos caracteres no evolucionados del concepto, donde se primaba la ejecución del tratamiento. De hecho, hay que recordar que, en la primera Ley federal alemana de 1977, se destacaba la operación de almacenamiento como elemento central, por lo que al responsable se le denominaba "organismo almacenante".

1.3.2. Aspectos concretos sobre los que recae la capacidad de determinar del responsable

La Directiva 95/46/CE establece que los aspectos concretos sobre los que el responsable ostenta la capacidad de determinar son "los fines y los medios del tratamiento". Hay leyes que contienen algunas divergencias respecto a estos aspectos[333], aunque algunas no los cambian de forma relevante[334].

---

de España, Italia, Polonia, Suecia y Liechtenstein. En la Ley italiana se indica "a quien competa […] la decisión". Por tanto, el elemento se definiría como la capacidad de decisión, de forma que además se liga con la competencia. Es decir, la entidad debe ser competente para decidir sobre los aspectos que se especifican.

[332] En el Diccionario de la lengua española, de la RAE, 22ª ed., se define "controlar", como "1. Ejercer el control, 2. Moderarse" y "establecer" como "1. Fundar, instituir, 2. Ordenar, mandar, decretar, 3. Dejar demostrado y firme un principio, una teoría, una idea, etc., 4. Avecindarse o fijar la residencia en alguna parte, 5. Abrir por cuenta propia un establecimiento mercantil o industrial". En la Ley irlandesa el elemento funcional se define como la capacidad de "controlar" (*control*), lo que hace más hincapié en la posibilidad de someter a otros a ese control. En la Ley rumana el elemento funcional es el término establecer en lugar de determinar.

[333] Estas Leyes son las de Estonia, Eslovaquia, Finlandia, Grecia, Hungría, Italia, Irlanda, Reino Unido, República Checa, Islandia y Liechtenstein. Si bien, ya se comentó lo referido a la Ley Húngara anteriormente que, en principio contiene los mismos aspectos contemplados por la Directiva 95/46/CE.

[334] En la Ley inglesa el elemento funcional sería la determinación de los fines y la manera en que los datos se tratan. La diferencia esencial respecto a la definición de la directiva es que, en vez de "medios" (*means)* se utiliza el término "manera" (*manner*). La Ley griega en lugar de fines y medios se refiere a "alcance y medios". En la Ley estonia los aspectos sobre los que se refleja la capacidad de determinación son: los fines del tratamiento de datos personales, las categorías de datos personales tratados, el procedimiento y la forma del tratamiento de datos personales y la autorización para comunicar datos personales a terceros. Este listado de elementos recuerda al listado que la primera propuesta de la Directiva 95/46/CE estableció (la Propuesta de Directiva de 1990) y que finalmente se redujeron. Como ya se comentó, el GA29 entendió que esta reducción no implicó una supresión de los elementos en el juego de determinación del responsable sino solamente un esfuerzo de simplificación. En el caso de la Ley islandesa la capacidad de determinar se refleja en los fines del tratamiento de datos personales, los medios que se utilizan, el método del tratamiento y otros usos de los datos. Por tanto, se añaden el método del tratamiento y otros usos de los datos. Sin embargo, tanto el método como los usos no parecen sino concreciones de los fines y los medios. La Ley

El GA29 interpretaba que los fines del tratamiento siempre debían ser determinados por el responsable. Respecto a los medios del tratamiento, el GA29 distinguía entre los esenciales, sobre los que necesariamente el responsable debe ejercer su capacidad de determinación, y los no esenciales. Sobre los medios no esenciales no era necesario que decidiera el responsable, sino que lo podía hacer también el encargado del tratamiento y se mencionaban, como ejemplo, los medios técnicos utilizados.

En este sentido, hay leyes que contienen importantes diferencias que afectan a los elementos considerados como esenciales para identificar al responsable, como la Ley finlandesa, en la que el poder de determinación se reduce al uso del fichero y no menciona la finalidad del mismo. La Ley italiana, especifica que uno de los aspectos sobre los que el responsable tendrá poder de determinación es el de las medidas de seguridad, aspecto que el GA29 *a priori* entendía como no esencial[335].

Algunas leyes, como la irlandesa, no consideran que los medios del tratamiento sean siquiera un elemento esencial[336]. Por último, las Leyes checa y eslovaca incluyen referencias al papel del responsable como tratador efectivo de los datos, es decir, como

---

eslovaca incluye los fines y los medios pero añade que el responsable determinará las condiciones del tratamiento de datos y que tratará datos personales. En cuanto al aspecto añadido relativo a las condiciones del tratamiento, la ley incluye una definición que parece ser una ampliación del término medios, de forma que se incluye todo lo que ayude a fijar los mismos, como requisitos, criterios o instrucciones. Por último, la legislación española también veremos que contiene diferencias respecto a estos aspectos.

[335] En la Ley italiana la capacidad de decisión del responsable se proyecta sobre "la finalidad, la modalidad de tratamiento de datos personales y los instrumentos utilizados, incluido todo lo relativo a las medidas de seguridad" (art. 4.f) Ley italiana). El GA29 ya mencionaba en su análisis que, en determinados sistemas jurídicos nacionales las decisiones entorno a las medidas de seguridad se consideraban elementos esenciales. De hecho, el GA29 especificaba que, en estos casos, debía tenerse en cuenta lo que establece la legislación nacional. Por tanto, parece claro que el GA29 se refería al caso italiano. Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.* pág. 16. Asimismo, como se apuntará en el caso español, aunque esto no aparezca expresamente en la definición de responsable, también puede entenderse que el poder de decisión sobre las medidas de seguridad será un aspecto esencial para determinar al mismo.

[336] La Ley irlandesa refleja la capacidad de control en el contenido y uso de los datos personales, no en los fines y los medios del tratamiento de datos personales. La referencia a contenido y uso de los datos, apunta a que lo que controla el responsable es qué datos manejará y el uso que se dará a estos. De nuevo hay que mencionar la Ley finlandesa, que sólo se refiere al uso del fichero. En la Ley de Liechtenstein el poder de decisión se refleja sobre la finalidad y el contenido del fichero. Por tanto, si bien la finalidad coincidiría con la regulación de la Directiva 95/46/CE (aunque ésta se refiriese al tratamiento) no coincide el otro elemento, el contenido. Al igual que la referencia al fichero, la mención al contenido responde a una noción menos evolucionada del responsable, donde es más importante la decisión sobre lo que contiene el fichero que los medios que se utilizan para tratar los datos.

sujeto que debe tratar los datos directamente, aunque entiendo que no puede interpretarse que ambas normas establezcan este rasgo como algo que caracterice al responsable[337].

1.3.3. El reenvío

La Directiva 95/46/CE, además de establecer los rasgos diferenciadores del responsable en el elemento funcional, tal como se ha comentado, y que se fundamentan en la capacidad de determinación que se refleja en los fines y los medios del tratamiento de datos, también permite que se defina quién ha de ser este responsable mediante las normas que establezcan los fines y los medios del tratamiento (art. 2.d) Directiva 95/46/CE). De esta forma, la ley podría designar directamente quien es responsable o podría hacerlo indirectamente, al establecer los criterios que servirían para determinarlo.

Este reenvío que contempla la Directiva 95/46/CE no se ha incluido en todas las leyes europeas[338]. Entiendo que el hecho de que no se haya incluido no impide que pueda, de todas formas, realizarse la designación del responsable en la legislación que establezca la obligación de tratar datos personales. El reenvío es más bien una pauta para el

[337] En la Ley checa el elemento funcional es de nuevo el verbo "determine" y los aspectos sobre los que se refleja esta capacidad son los fines y medios (del tratamiento de datos personales). Hasta aquí el elemento es idéntico al de la Directiva 95/46/CE. No obstante, en la definición de la ley checa se añade que lo lleve a cabo (el tratamiento) y que sea responsable (del tratamiento). Estos dos aspectos añadidos parecen dar a entender que para que se considere a una entidad como responsable deberá determinar los fines y los medios, llevar a cabo el tratamiento y ser responsable. El hecho de precisar que el sujeto debe ser responsable es confuso y, al incluirse la precisión de que debe llevar a cabo el tratamiento implica que tendrá que ser un tratador efectivo de los datos, lo que parece responder a una definición arcaica de responsable. Sin embargo, a continuación se establece la posibilidad de que el responsable no realice ese tratamiento cuando se indica que podrá apoderar a un encargado del tratamiento para que realice el tratamiento. Por lo tanto, el rasgo de tratador efectivo no puede ser característico del responsable, quien puede delegar esta gestión en otro. La Ley eslovaca incluye en el concepto de responsable el requisito de que trate los datos en su propio nombre. Esta exigencia se añade a la necesidad de que determine los fines, los medios y las condiciones del tratamiento de datos. Sin embargo, entiendo que esta ley exige que sólo pueden tratar datos de forma autónoma los que sean responsables del tratamiento y esto es lo que se refleja en la definición. Hay que tener en cuenta que es la ley más moderna de las analizadas y en ella se aprecia una evolución en la concepción de la regulación. Por eso, no parece lógico que este requisito aludiera a la exigencia de que el responsable fuera un tratador efectivo, característica que pertenece a conceptos poco desarrollados.

[338] Las leyes donde se ha establecido este reenvío son las Leyes de Bélgica, Bulgaria, Croacia, Eslovenia, Eslovaquia, Finlandia, Francia, Grecia, Hungría, Letonia, Lituania, Luxemburgo, Portugal, Reino Unido y Rumanía. No se ha establecido el reenvío en las Leyes de Alemania, Chipre, Dinamarca, España, Estonia, Países Bajos, Italia, Irlanda, Malta, Polonia, República Checa, Suecia, Islandia, Liechtenstein y Noruega. Si bien hay que mencionar que en el artículo 20 de la Ley de Liechtenstein, se establece que si una autoridad trata datos juntamente con otras autoridades o con personas privadas, el gobierno podrá regular las responsabilidades específicas en materia de protección de datos. Por tanto, se especifica que en el marco del sector público podrá establecerse una regulación para los casos en los que se prevea que exista una corresponsabilidad para delimitar las responsabilidades. No se incluye, sin embargo, una previsión similar para el sector privado.

legislador, por lo que no parece preciso incorporarla en la normativa nacional para poder utilizarlo.

En las normas en las que sí se introduce este reenvío, no en todos los casos se ha respetado la literalidad del precepto de la Directiva 95/46/CE. Una de la cuestiones que se modifica es la tipología de la norma a la que se reenvía que, si bien, en algunas leyes se describe de forma neutra, en otras se intenta amoldar a las características del sistema legal del Estado[339].

Hay que destacar las Leyes francesa y finlandesa en las que se establecen dos vías para determinar al responsable: que la ley lo designe o que se apliquen los elementos del concepto[340]. Es decir, estas leyes no exigen expresamente que la designación en la ley del responsable sea consecuencia de que ésta establezca los fines y los medios del tratamiento. Por tanto, es una modificación sustancial del concepto, tal como se establece en la Directiva 95/46/CE y además iría en contra de la interpretación del GA29, que prima el hecho de que se determinen realmente los fines y medios del tratamiento, por encima de una designación meramente formal. No obstante, podrían interpretarse estas remisiones, en el mismo sentido que la Directiva 95/46/CE y exigir que la designación se conecte con el establecimiento de los fines y los medios en la ley.

Encontramos diferencias en algunas leyes respecto a los aspectos que debe determinar la ley para proceder a la designación del responsable[341]. Además, no todas las

[339] En las Leyes de Bulgaria, Croacia, Eslovenia. Finlandia se alude simplemente a la ley. En las Leyes francesa, griega, lituana, luxemburguesa, inglesa y rumana la alusión es también neutra y se alude en casi todas a los términos "disposiciones legales". La Ley belga ha sustituido la referencia a las fuentes normativas indicadas por los tipos de normas que se ajustan al ordenamiento belga (una ley, un decreto, una ordenanza). La Ley eslovaca se refiere a una ley específica, una norma directamente aplicable y legalmente vinculante de la Unión Europea o un tratado internacional que obligue a la República de Eslovaquia.

[340] Así la Ley finlandesa establece que "Responsable del tratamiento es una persona, empresa, institución o fundación, o varias de ellas, para quienes, con el fin de que lo utilicen, se establece un fichero y quienes están capacitadas para determinar el uso del fichero, o quienes hayan sido designadas como responsables por una ley". La Ley francesa incluye la siguiente definición: "El responsable de un tratamiento de datos de carácter personal es, salvo designación expresa por las disposiciones legislativas o reglamentarias relativas a este tratamiento, la persona, la autoridad pública, el servicio o el organismo que determina sus finalidades y sus medios".

[341] Las Leyes búlgara, húngara y eslovaca, cuando se refieren a los aspectos que debe establecer la ley para poder realizar la designación del responsable, añaden algunos distintos a los fines y los medios del tratamiento. La Ley lituana, en vez de aludir a los fines y los medios del tratamiento como presupuesto para poder designar al responsable, se limita a mencionar la necesidad de que se determinen los fines del mismo. Al igual sucede en la Ley inglesa que sólo se refiere a los fines como aspecto que se determinará en la ley de la que emana la obligación del tratamiento. La Ley eslovaca menciona la finalidad o las condiciones del

leyes que incluyen este reenvío respetan las dos opciones de designación directa e indirecta que prevé la Directiva 95/46/CE[342].

En algún caso la ley establece que la designación del responsable debe realizarse en la ley que establezca la organización o el funcionamiento o en los estatutos que rijan el órgano jurídico competente para tratar los datos[343]. Sin embargo, algunas leyes tergiversan el reenvío, de forma que enlazan con supuestos de legitimación del tratamiento, como son la necesidad de tratar datos para cumplir con una obligación legal o para llevar a cabo una competencia administrativa[344].

También cabe mencionar el caso peculiar de la Ley letona que realiza un reenvío a la propia ley de protección de datos, lo que modifica la finalidad de este mecanismo[345].

1.3.4. Corresponsabilidad

El artículo 2.d) Directiva 95/46/CE incluía en la definición del responsable del tratamiento que éste podía actuar "solo o conjuntamente con otros", lo que implica la posibilidad de que existan varios responsables que determinen los fines y los medios del

---

tratamiento como los aspectos que pueden establecerse en la ley y que darán lugar a la designación del responsable.

[342] Las Leyes de Croacia, Eslovenia, Finlandia, Francia, Hungría, Portugal, Reino Unido y Rumanía sólo contemplan la posibilidad de designación directa del responsable. Respetan las dos opciones las Leyes búlgara, belga, eslovaca, griega y lituana. Una última variación la presenta la Ley luxemburguesa que ofrece sólo la opción relativa a la fijación de los criterios específicos para la designación del responsable y no la designación directa del mismo.

[343] La Ley portuguesa indica que "en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias, el responsable del tratamiento será designado en la ley que establezca la organización o el funcionamiento o en los estatutos que rijan el órgano jurídico o estatutario competente para tratar los datos".

[344] En la Ley inglesa, el reenvío se contempla en la subsección 4, a la que remite la definición de responsable e indica que "cuando los datos personales se tratan sólo para fines para los que por o en virtud de una disposición legal es preciso que se traten, la persona en quien recaiga la obligación de tratar los datos que se impone por o en virtud de la disposición legal será a los efectos de esta ley considerado responsable del tratamiento. En la Ley húngara el reenvío no se encuentra en la definición de responsable. Este reenvío se encuentra en otro precepto de la ley, la Sección 5.3 que versa sobre la legitimación del tratamiento de datos. Establece esta disposición que la norma donde se podrá realizar la designación del responsable es la norma o el decreto municipal de donde emane la obligación de realizar el tratamiento. Aunque si se trata de una norma local, la autoridad de quien proceda esta norma deberá estar autorizada por ley y ligarse al cumplimiento de tareas que persigan el interés público.

[345] La Ley letona define al responsable como "la persona física o jurídica, institución del gobierno estatal o local que determina los fines y los medios del tratamiento de datos personales y que es responsable por el tratamiento de datos personales de acuerdo con esta ley" (el subrayado es de la autora). Por tanto, en lo que respecta al reenvío se ha transformado, de forma que se remite como un criterio añadido para definir al responsable a lo que establezca la ley de protección de datos.

tratamiento de datos personales. Pues bien, este aspecto que refleja la posibilidad expresa de contemplar los supuestos de corresponsabilidad y que, por tanto, ha adquirido una gran importancia en el actual contexto tecnológico, debido a la complejidad de los modelos y estructuras negociales y organizativas, se incluye en poco más de la mitad de las leyes analizadas[346].

1.4. Importantes divergencias como resultado del análisis comparativo

Como se ha podido observar del análisis realizado existen muchas diferencias. Si bien la mayoría de estas diferencias son superables con una interpretación que esté en línea con lo establecido por la Directiva 95/46/CE, existen otras de más envergadura que difícilmente podrán superarse con esta interpretación. Como ejemplos cabe citar: la definición de la ley alemana que se refiere claramente a un responsable que es un tratador efectivo de los datos y que no tiene en cuenta la capacidad de determinar el tratamiento (elemento funcional) para definir a este sujeto; las leyes que en sus definiciones admiten que puedan ser responsables sujetos sin personalidad jurídica o cuando el elemento objetivo es el fichero en lugar del tratamiento de datos personales.

Estas diferencias hacen muy difícil que en los diversos Estados miembros un mismo responsable, aplicando los criterios que se proporcionan en las leyes nacionales, pueda llegar al mismo resultado en la determinación de si se considera o no responsable del tratamiento. Asimismo, el hecho de tener que depender de un proceso de interpretación, en línea con la directiva, crea necesariamente una debilidad en la regulación. Estas dificultades irían en contra del objetivo de la Directiva 95/46/CE que, precisamente, es armonizar la aplicación del concepto e interpretarlo de acuerdo con el derecho comunitario en su calidad de concepto autónomo, con el fin de facilitar la libre circulación de datos personales en el mercado interior y lo que harían es crear el efecto

[346] Sí lo han hecho las Leyes de Austria, Bélgica, Bulgaria, Dinamarca, Eslovenia, Eslovaquia, España, Finlandia, Países Bajos, Hungría, Italia, Irlanda, Lituania, Luxemburgo, Malta, Portugal, Reino Unido y Suecia. Hay que resaltar la Ley austríaca, en la que se va más allá, al regular la figura del "sistema conjunto de información" que incluso implica la designación de un operador que tendrá una serie de obligaciones. En la Ley inglesa se utilizan dos fórmulas "*jointly*" y "*in common*" para hacer referencia a la corresponsabilidad, mientras que en la directiva sólo se utiliza la primera. No se incluye este aspecto de la corresponsabilidad en las Leyes de Alemania, Chipre, Croacia, Estonia, Francia, Grecia, Letonia, Polonia, República Checa, Rumanía, Islandia, Liechtenstein y Noruega. No obstante, respecto a la Ley alemana hay que indicar que luego en la regulación (art. 6.2 y 8 Ley alemana) sí que se ha tenido en cuenta esta posibilidad desde la perspectiva del interesado.

contrario. Así lo señaló, también, la Comisión Europea en un estudio realizado a propósito de la reforma de la Directiva 95/46/CE[347].

2. LA RECEPCIÓN DEL CONCEPTO DE RESPONSABLE EN LA LEGISLACIÓN ESPAÑOLA DE PROTECCIÓN DE DATOS

Antes de proceder al análisis del concepto de responsable en la legislación española, se hará una breve referencia a la Constitución Española en la que se plasmó un mandato al legislador para proteger a los ciudadanos del uso de la informática. Este mandato dio lugar al reconocimiento por el Tribunal Constitucional del derecho a la protección de datos, que confirmó, así, la importancia de esta legislación en nuestro país.

2.1. La limitación del uso de la informática en la Constitución Española y el reconocimiento del derecho a la protección de datos por el Tribunal Constitucional

Si bien la Constitución Española no contempla de forma expresa el derecho a la protección de datos personales, en el artículo 18.4 CE contiene un mandato al legislador, inspirado en el artículo 35 de la Constitución portuguesa[348], la primera que reconoció de forma expresa, el derecho a la protección de datos[349]: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

---

[347] Así lo indica también la Comisión en el estudio de impacto realizado a raíz de la preparación de la reforma de la Directiva 95/46/CE donde señala algunas de las diferencias existentes en los conceptos de responsable del tratamiento en las leyes de los Estados miembros. La Comisión subraya el papel crucial que desempeña este concepto, junto al de encargado del tratamiento para determinar la responsabilidad por el cumplimiento con las reglas establecidas, el ejercicio de los derechos de los interesados, la ley nacional aplicable y el control realizado por las autoridades de control. Las interpretaciones divergentes con relación a estos conceptos originan efectos negativos en la protección de los datos y un coste añadido para el responsable que se encuentra establecido en varios Estados miembros y debe adaptarse a las diferentes interpretaciones. Se señala en el estudio la especial importancia de que no se contemplen en las leyes nacionales las fórmulas de corresponsabilidad, ya que las tendencias económicas y tecnológicas implican que exista cada vez más este supuesto. *Commission Staff Working Paper, Impact assessment accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*. *SEC(2012) 72 final, Brussels, 25.1.2012, Annex 2*, págs. 16 a 19.

[348] O. ALZAGA VILLAAMIL, *Comentario sistemático a la Constitución Española de 1978*, Ediciones del Foro, Madrid, 1979, págs. 209 a 210.

[349] A. TRONCOSO REIGADA, *La protección de datos personales. En busca del equilibrio*, *op. cit.*, pág. 49.

Esta disposición ha sido objeto de interpretaciones doctrinales divergentes en cuanto a si debía considerarse que este mandato implicaba la ampliación del derecho a la intimidad o un derecho nuevo y distinto de los establecidos por el artículo 18 CE[350]. Finalmente, el Tribunal Constitucional, que había emitido sentencias algo titubeantes acerca de esta materia[351], zanjó el debate doctrinal mediante dos importantes sentencias: la STC 290/2000 y, especialmente, la STC 292/2000, ambas de 30 de noviembre de 2000[352]. En ellas establece claramente la existencia de un derecho a la protección de datos personales y, además, perfila sus principales características.

[350] ARENAS RAMIRO menciona como defensores de la tesis de que el 18.4 CE es una ampliación del derecho a la intimidad a ORTI VALLEJO, RUÍZ MIGUEL y GRIMALT SERVERA. De otro lado, como defensores de la tesis de que el 18.4 CE implica la existencia de un derecho autónomo del de la intimidad, MURILLO DE LA CUEVA, GÓNZALEZ MURÚA y PÉREZ LUÑO. M. ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa, op. cit.*, pág. 456.

[351] Ejemplo de estas sentencias es la STC 254/1993, de 20 de julio de 1993, FJ 6, que hace referencia a una nueva garantía constitucional incorporada en el 18.4 CE, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama "la informática". No obstante, el Tribunal en el resto de la fundamentación se refiere al derecho a la intimidad, incluso cuando menciona por primera vez la "libertad informática" o *habeas data*, indicando que la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. HERNÁNDEZ LÓPEZ distingue tres fases en la jurisprudencia del Tribunal Constitucional relativa al derecho de protección de datos de carácter personal. La etapa inicial de 1981 a 1993 en la que destaca la preocupación por los peligros de las nuevas tecnologías y su incidencia en los derechos fundamentales, la etapa de transición de 1993 a 2000 (donde se incluiría como sentencia clave la comentada STC 254/1993), donde la "libertad informática" es la expresión positiva del derecho a la intimidad y la fase de reconocimiento pleno de 2000 hasta la actualidad, J.M. HERNÁNDEZ LÓPEZ, *El derecho a la protección de datos personales en la doctrina del Tribunal Constitucional*, Aranzadi, 2013, Cizur Menor (Navarra), págs. 87 a 111.

[352] La STC 290/2000 respondió a cuatro recursos de inconstitucionalidad interpuestos contra la LORTAD por el Defensor del Pueblo, por 56 diputados del Grupo Parlamentario Popular y por el Consejo Ejecutivo y el Parlamento de Cataluña contra los artículos 6.2, 19.1, 20.3, 22.1 y 2.1, 24, 31, 39.1 y 2, 40.1 y 2 y Disposición final tercera de la LORTAD. La STC 292/2000 fue originada por un recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo contra ciertos incisos de los artículos 21.1 y 24.1 y 2 de la LOPD, cuya Disposición final segunda les privaba de la forma de Ley Orgánica ya que, entendía que vulneraban la reserva de ley del artículo 53.1CE, el artículo 18.1 y 4 CE, al no respetar el contenido esencial del derecho fundamental al honor y a la intimidad personal y familiar, así como del derecho fundamental denominado de "libertad informática", de acuerdo con las SSTC 254/1993, de 20 de julio, 94/1998, de 4 de mayo, y 202/1999, de 8 de noviembre. Ambas sentencias se resuelven el mismo día, el 30 de noviembre de 2000, pese a que la STC 290/2000 responde a unos recursos que se interpusieron en enero de 1993. La LOPD inició su trámite parlamentario como un proyecto de ley orgánica de modificación parcial de la LORTAD para adaptarla a la Directiva 95/46/CE. Sin embargo, finalmente, se aprobó una nueva ley que era muy similar a la LORTAD, que fue derogada. De esta forma, parecía que lo que pretendían los artífices de esta maniobra (el partido que en ese momento ostentaba el poder era el Grupo Popular) era esquivar la declaración de inconstitucionalidad de la LORTAD. El Tribunal Constitucional opta por emitir dos sentencias, la 290/2000 referida a la LORTAD, donde se pronuncia sobre los aspectos competenciales e institucionales, quedando sin objeto el resto de cuestiones sustantivas. Las cuestiones sustantivas las aborda el Tribunal Constitucional en su sentencia 292/2000 referida a la LOPD. P. LUCAS MURILLO DE LA CUEVA "La primera jurisprudencia sobre el derecho a la autodeterminación informativa", *Datospersonales.org*, nº 1, Marzo 2003.

El Tribunal Constitucional se remonta al proceso de elaboración de la Constitución para tener en cuenta que el constituyente fue consciente de los riesgos que podía entrañar el uso de la informática. Por ese motivo, se incorporó, mediante el artículo 18.4 CE, un instituto de garantía como forma de respuesta a una nueva forma de amenaza a la dignidad y a los derechos de la persona pero que es también, en sí mismo, un derecho o libertad fundamental[353]. Como se indica en la sentencia, en el Senado se suscitaron dudas sobre si era necesario incluir el inciso final de este artículo 18.4 CE ("y el pleno ejercicio de sus derechos"). Este inciso transformó esta disposición que, en principio, sólo iba a referirse a la protección de los concretos derechos al honor y la intimidad personal y familiar, para extender esta protección al pleno ejercicio de los derechos de la persona[354]. El derecho que se reconoce posee un carácter instrumental, ya que permite garantizar otros derechos[355].

El Tribunal Constitucional distingue el derecho a la protección de datos del derecho a la intimidad, ya que les atribuye una función distinta que hace que también su objeto y contenido difieran. En palabras del tribunal:

> "la función del derecho a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad. En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado" (STC 292/2000, de 30 de noviembre de 2000, FJ 6).

[353] STC 292/2000, de 30 de noviembre de 2000, FJ 4, que hace referencia a su vez a la STC 254/1993, de 20 de julio, FJ 6.
[354] STC 292/2000, de 30 de noviembre de 2000, FFJJ 4 y 6.
[355] Muestra de este carácter instrumental es la STC 11/1998, de 13 de enero de 1998 y una larga lista de sentencias del Tribunal Constitucional referidas a un mismo supuesto de utilización por parte de la empresa pública RENFE de su fichero de datos sobre filiación sindical para detraerles a los trabajadores de un sindicato que había convocado una huelga la parte proporcional de su salario correspondiente a la duración de la misma. Se trata de casos en los que estos trabajadores ni siquiera secundaron la huelga o no pudieron hacerlo porque se realizó fuera de su jornada laboral. La STC 11/1998 se refiere a la STC 254/1993 en cuanto al reconocimiento del derecho a la libertad informática en su FJ 7 pero además añade en su FJ 5: "En efecto, el art. 18.4 en su último inciso establece las limitaciones al uso de la informática para garantizar el pleno ejercicio de los derechos, lo que significa que, en supuestos como el presente, el artículo citado es, por así decirlo, un derecho instrumental ordenado a la protección de otros derechos fundamentales, entre los que se encuentra, desde luego, la libertad sindical, entendida ésta en el sentido que ha sido establecido por la doctrina de este Tribunal, porque es, en definitiva, el derecho que aquí se ha vulnerado como consecuencia de la detracción de salarios, decidida por la empresa al trabajador recurrente por su incorporación a determinado Sindicato."

Por lo tanto, el objeto del derecho a la protección de datos es más amplio que el del derecho a la intimidad, ya que no se limita a los datos considerados íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por un tercero pueda afectar a sus derechos, sean o no fundamentales[356]. Se trata de proteger cualquier dato que identifique o permita identificar a una persona y que pueda servir para la confección de un perfil de esa persona o para cualquier utilidad que pueda suponer una amenaza para el individuo[357].

El contenido también difiere en ambos derechos. El derecho a la intimidad permite a la persona imponer a terceros el deber de abstenerse de toda intromisión en su esfera íntima. En cambio, el derecho a la protección de datos atribuye a su titular un haz de facultades cuyo ejercicio impone a terceros deberes jurídicos, que permiten garantizar a esa persona el poder de disposición sobre sus datos personales. Por lo tanto, estamos ante las dos caras de la moneda: el haz de facultades que el derecho atribuye a los titulares y las obligaciones que se instauran para los terceros, sean el Estado o un particular, que tratan esos datos. Estas facultades se concretan según el Alto Tribunal en:

> "la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento,

[356] PARDO alerta precisamente del peligro que supone la omnipresencia de la protección de datos para derechos tradicionales como el de intimidad, la propia imagen o el secreto de comunicaciones. Así, esta autora indica de forma gráfica que "los datos lo invaden todo y dificultan a los juristas la vista del rico y variado bosque de los derechos fundamentales en su conjunto. Lo que en sus orígenes era para muchos un "medio" ha terminado por convertirse no ya en "fin" sino en fin casi absoluto (si siguen así las cosas) que amenaza con devorar a otros derechos de larga tradición ahora arrinconados". M. M. PARDO LÓPEZ, "No sólo protección de datos personales en Internet: de los conceptos jurídicos híbridos, las categorías mutantes y otras evoluciones en curso", J. VALERO TORRIJOS (Coord), VVAA, *La protección de los datos personales en Internet ante la innovación tecnológica. Riesgos, amenazas y respuestas desde la perspectiva jurídica*, Aranzadi, Cizur Menor (Navarra), 2013, pág. 101. También GRIMALT SERVERA se refiere a los efectos expansivos de la aprobación de la LOPD, de forma que considera que los conceptos de tratamiento y de dato personal que establece son tan amplios que han configurado a esta ley como norma general de tratamientos de datos que además no se limitaría a proteger unos bienes jurídicos concretos, sino que protegería los datos *per se*. En consecuencia, para GRIMALT SERVERA, esto implica que frente a la regulación general de protección de datos, exista la regulación específica referida a bienes jurídicos concretos (la intimidad, el honor y la propia imagen) que se contiene en la LO 1/1982 y que, al ser ley especial respecto a la LOPD, será de aplicación preferente en caso de protección civil de estos bienes jurídicos concretos. No obstante, este autor indica que la LOPD se aplicará también cuando se vulneren los derechos a la intimidad, al honor y a la propia imagen pero su aplicación se limitará a la protección administrativa. P. GRIMALT SERVERA, "La necesaria reconducción del régimen jurídico de la protección de los datos personales desde la perspectiva de los conflictos y solapamientos con otros derechos y libertades en Internet", J. VALERO TORRIJOS (Coord), VVAA, *La protección de los datos personales en Internet ante la innovación tecnológica. Riesgos, amenazas y respuestas desde la perspectiva jurídica*, *op. cit.*, págs. 74 a 75.

[357] STC 292/2000, de 30 de noviembre de 2000, FJ 6.

> informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo y, por otro lado, el poder oponerse a esa posesión y usos" (STC 292/2000, de 30 de noviembre de 2000, FFJJ 6 y 7).

El Tribunal Constitucional, además, confirma sus conclusiones con la alusión a los diversos textos legales existentes, que se han recorrido en el presente trabajo. Y es que la afirmación rotunda de la existencia del derecho a la protección de datos se ve apoyada por el reconocimiento externo de la Carta UE que, como ya se ha visto, fue aprobada a nivel interinstitucional unos días después de que se emitieran estas sentencias[358].

Queda claro el reconocimiento del derecho a la protección de datos, como un derecho fundamental autónomo, que implica unas obligaciones para los sujetos que tratan datos para poder asegurar el poder de disposición de los titulares de los datos. Asimismo, pese a que el derecho a la protección de datos se haya construido jurisprudencialmente, encuentra su anclaje en la Constitución. Esto implica que el derecho disfruta de la eficacia vinculante de la Constitución respecto a los poderes públicos y también respecto a los ciudadanos[359].

Sin embargo, este derecho no es absoluto y sus límites hay que encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, en virtud del principio de unidad de la Constitución. Estos límites deberán cumplir tres condiciones: primera, estar establecidos por ley (arts. 53.1 y 81 CE); segunda, responder a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos, si el límite es necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo; y, tercera, deben respetar el contenido esencial del derecho de protección de datos que se

[358] El Tribunal alude concretamente en su STC 292/2000 de 30 de noviembre de 2000, FJ 8, a la Resolución 45/95 de la Asamblea General de las Naciones Unidas que recoge los Principios rectores aplicables a los ficheros computadorizados de datos personales, al Convenio 108, a la Directiva 95/46/CE y a la Carta UE y entiende que todos estos textos "coinciden en el establecimiento de un régimen jurídico para la protección de datos personales en el que se regula el ejercicio de este derecho fundamental en cuanto a la recogida de tales datos, la información de los interesados sobre su origen y destino, la facultad de rectificación y cancelación, así como el consentimiento respecto su uso o cesión." Lo que se traduce en el haz de garantías que hace posible el respeto del derecho fundamental.

[359] El artículo 9.1 CE establece: "Los ciudadanos y los poderes públicos están sujetos a la Constitución y al resto del ordenamiento jurídico". Refleja, de esta forma, esta disposición, la tesis germana del *Drittwirkung*, A.E. PÉREZ LUÑO, *Derechos humanos, estado de derecho y constitución*, 10ª ed., Tecnos, Madrid, 2010, pág. 333.

extiende al conjunto de garantías y facultades que conforman el poder de disposición sobre la información personal[360].

En todo caso, la regulación de este contenido del derecho fundamental se incluyó, primero, en la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), que fue sustituida por la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD)[361].

2.2. La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal

Si bien esta norma se aprobó antes del claro reconocimiento por el Tribunal Constitucional de la existencia del derecho a la protección de datos, su exposición de motivos curiosamente, no se refería a la protección de datos sino a la noción de privacidad, y la definía sin ambages, en contraposición a la noción de intimidad. Si la intimidad protegía la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona, la privacidad constituía un conjunto más amplio de facetas de su personalidad que, aisladamente consideradas, podían carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojaban como precipitado un retrato de la personalidad del individuo que éste tenía derecho a mantener reservado.

La LORTAD se aprobó por exigencias del Acuerdo de Schengen[362] y en su proceso de elaboración se tomó como referencia el texto de la Propuesta de Directiva de

[360] STC 292/2000, de 30 de noviembre de 2000, FJ 11. A. TRONCOSO REIGADA, *La protección de datos personales. En busca del equilibrio*, *op. cit.*, págs. 141 a 142.

[361] Cabe mencionar también la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho a la intimidad personal y familiar y a la propia imagen, que en su disposición transitoria primera señalaba: "En tanto no se promulgue la normativa prevista en el artículo 18.4 de la Constitución, la protección civil del honor y la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática se regulará por la presente ley.". Por tanto, antes de la aprobación de la LORTAD, la ley mencionada fue el texto utilizado para proteger las vulneraciones cometidas por el uso de la informática, aunque sólo con relación a la vulneración del derecho a la intimidad o al honor, con las connotaciones que ello tenía para su protección, como indicó el Tribunal Constitucional en las sentencias mencionadas. Esta norma evidentemente no regula la figura del responsable, pero protege frente a las intromisiones ilegítimas que puedan realizar a estos derechos tanto el sector público, como el privado.

[362] Así lo manifiesta la Sra. De Palacio Valle-Lersundi, del Grupo Popular en el debate parlamentario sobre las enmiendas a la totalidad de la LORTAD: "y ahora, no nos engañemos, es el mandato urgente del

1990 y el Convenio 108. Esto implicó que tuviera que aprobarse una nueva ley que se adaptara al texto final de la Directiva 95/46/CE, la LOPD[363].

El responsable se definió en la LORTAD como: "Responsable del fichero: persona física, jurídica de naturaleza pública o privada y órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento" (art. 3.d LORTAD).

Lo primero que se observa es que se le denominaba "responsable del fichero", lo que se importó claramente de la Propuesta de Directiva de 1990. Asimismo, de acuerdo con la metodología de análisis seguida, hasta ahora, el elemento subjetivo se describía como "persona física, jurídica de naturaleza pública o privada y órgano administrativo", el elemento objetivo: "el tratamiento" y el elemento funcional "que decida" que se proyecta sobre la "la finalidad, contenido y uso" del tratamiento. La definición permaneció inalterable durante el proceso parlamentario de elaboración de la norma. La LORTAD se desarrolló reglamentariamente pero en estas regulaciones no se especificaba nada sobre el concepto del responsable del fichero[364]. A continuación se procede al análisis de estos elementos.

Acuerdo de Schengen el que reclama que en el momento de entrar en vigor ese propio Acuerdo de Schengen, exista ya una normativa desarrollada en todos los países signatarios que regule y desarrolle el Convenio de Estrasburgo, el Convenio del Consejo de Europa." Debate de totalidad del Proyecto de Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal. "Boletín Oficial de las Cortes Generales", Serie A, número 59.1, de 24 de julio de 1991 (número de expediente 121/000059). Cortes Generales, Diario de Sesiones del Congreso de los Diputados, Pleno y diputación permanente, IV Legislatura, núm. 145, sesión plenaria del 28 de noviembre de 1991, pág. 7584. De hecho, en esa misma sesión se debatían las enmiendas a la totalidad del Acuerdo Schengen, págs. 7525 a 7532.

[363] De hecho el Sr. Santos Miñón, del grupo CDS, como un argumento para apoyar su enmienda a la totalidad, esgrime el hecho de que la propuesta de directiva aún esté en su primera vuelta: "Presentar un proyecto de ley que antes de ser aprobado ya tiene su muerte –al menos parcial- anunciada, debe considerarse un dislate, aún en el caso de que se hayan seguido las líneas generales de la mencionada Directiva, pues el texto de la misma ha producido ya varias reacciones, estando como está en la primera vuelta. Así, UNICE y el Informe Herman hacen prever la introducción de modificaciones importantes antes de su aprobación definitiva.", Debate de totalidad del Proyecto de Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal, *op. cit.*, pág. 7580.

[364] Los desarrollos reglamentarios se realizaron mediante las siguientes disposiciones: Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, Real Decreto 1332/94 de 20 de junio, por el que se desarrollan algunos preceptos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal y Real Decreto 994/1999, de 11 de junio, por el que se aprueba el reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

2.2.1. El elemento subjetivo

El elemento subjetivo se describía como "persona física, jurídica de naturaleza pública o privada y órgano administrativo". Se incluían, por tanto, sujetos que pretendían cubrir, tanto el sector público como el privado, ya que la ley estableció, al igual que la Propuesta de Directiva de 1990, una doble regulación, que diferenciaba los dos sectores. Como ya se ha analizado anteriormente, esa dualidad desapareció posteriormente en la Directiva 95/46/CE. De hecho, una de las primeras críticas que recibió esta ley durante su proceso de elaboración, además de la polémica independencia de la AEPD, fue la diferenciación en la regulación de los ficheros que detentaba la administración pública y los que detentaba el sector privado.

Prácticamente, todos los partidos consideraron que se otorgaban mayores libertades a la administración para poder tratar datos. El gobierno se defendió con el argumento de que la administración ya tenía controles suficientes, como era la limitación en su actuación por las leyes, la necesidad de que se aprobara una disposición general para poder crear los ficheros o que se sometiera al control judicial. Por el contrario, el gobierno apuntó a que el mayor riesgo estaba en el sector privado, más difícil de controlar[365]. Así quedó finalmente reflejado en su exposición de motivos[366].

El debate parlamentario, durante el proceso de elaboración de la LORTAD, nos da una idea del contexto tecnológico incipiente en ese momento, cuando un diputado sugería

[365] Así lo argumentaba el Ministro de Justicia del momento, el Sr. De la Quadra-Salcedo y Fernández del Castillo, en el debate parlamentario sobre las enmiendas a la totalidad de la LORTAD. La Sra. De Palacio Valle-Lersundi, del Grupo Popular, cuestionaba, por el contrario, la doble regulación de los ficheros: "El proyecto de ley plantea una doble moralidad en cuanto a la valoración de los ficheros"[…]"los ficheros que están en manos de la Administración son mucho más potentes, tienen muchas más posibilidades y mucha más capacidad en sus manos para poder inmiscuirse y en un momento dado vulnerar esos derechos fundamentales de las personas." Debate de totalidad del Proyecto de Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal, *op. cit.*, págs. 7576 y 7585.

[366] El punto 4 de la exposición de motivos de la LORTAD indicaba: "Para la articulación de los extremos concretos que han de regir los ficheros de datos, la parte especial de la Ley comienza distinguiendo, en su Título Cuarto, entre los distintos tipos de ficheros, según sea su titularidad pública o privada. Con la pretensión de evitar una perniciosa burocratización, la Ley ha desechado el establecimiento de supuestos como la autorización previa o la inscripción constitutiva en un registro. Simultáneamente, ha establecido regímenes diferenciados para los ficheros en razón de su titularidad, toda vez que, con toda evidencia, resulta más problemático el control de los de titularidad privada que el de aquéllos de titularidad pública. En efecto, en lo relativo a estos últimos, no basta la mera voluntad del responsable del fichero sino que es precisa norma habilitante, naturalmente pública y sometida al control jurisdiccional, para crearlos y explotarlos, siendo en estos supuestos el informe previo del órgano de tutela el cauce idóneo para controlar la adecuación de la explotación a las exigencias legales y recomendar, en su caso, las medidas pertinentes."

que, para proteger los datos la policía no los introdujera en un fichero automatizado[367], o en el que se hizo mención de los ordenadores que utilizaban algunas administraciones y grandes empresas, herramientas que aún no estaban al alcance de todos[368]. De hecho, se puso de relieve en el debate que los ciudadanos aún no eran conscientes de los peligros de la utilización de la informática y se comparó ese momento con la etapa de la industrialización, en la que tampoco se fue consciente del peligro ecológico que ésta iba a suponer más adelante[369].

2.2.2. El elemento objetivo y el elemento funcional

La LORTAD establecía su aplicación "a los datos de carácter personal que figuren en ficheros automatizados de los sectores público y privado y a toda modalidad de uso posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado" (art. 2.1 LORTAD). Por tanto, la ley se refería al concepto de fichero automatizado, si bien el último inciso se interpretó que permitía la aplicación a algunos ficheros manuales[370]. No obstante, no se podía asimilar a

[367] Es el Sr. Nuñez Casal, del Grupo Izquierda Unida-Iniciativa per Catalunya, el que muestra gráficamente ese estadio:"Yo no he dicho que en el segundo nivel de protección, es decir, en aquellos datos que no hacen referencia al artículo 16, la policía o los jueces no puedan tener los datos. ¡Claro que los pueden tener, si hace falta, para la investigación del delito! Yo lo que he dicho es que esos datos no pueden estar informatizados, porque no hace falta que lo estén." […]" ¿Es que no sabe usted, señor Ministro, que, a pesar de que usted está en el Ministerio, los sistemas informáticos todavía brillan por su ausencia en montones de juzgados, aparte de que algunos quedan tirados en los pasillos porque no se han hecho los cursillos de formación necesarios? ¿Es que no hay montones de jueces que están actuando e investigando con esos datos y tienen, además a la policía con esos datos, sin necesidad de informatizarlos?"[…]"El dato se puede poseer, con el control judicial, pero no se puede informatizar, porque si no, señor Ministro, empiezan a ocurrir esas cosas que pasan."[…]"Nadie está en contra del avance tecnológico. Lo que se quiere es plantear una relación correcta entre lo que es avance tecnológico y lo que es protección jurídica", Debate de totalidad del Proyecto de Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal, *op. cit.*, pág. 7595.

[368] El Sr. Santos Miñón, de CDS enumera algunos de estos grandes ordenadores: "Berta", ordenador central de la Policía, "Duque de Ahumada", ordenador de la Guardia Civil o "Rita", ordenador de Economía y Hacienda. Debate de totalidad del Proyecto de Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal, *op. cit.*, pág. 7580.

[369] La Sra. De Palacio Valle-Lersundi, Grupo Popular, manifiesta que "Estos peligros, estos riesgos quizá no son percibidos con toda su gravedad por los ciudadanos españoles en este momento, un poco también como ocurrió en su día con la gran industrialización, cuando la gente no percibió los problemas y los graves peligros ecológicos de destrucción del medio ambiente que se iban creando en ese momento, y que luego han dado lugar a reacciones airadas e incluso violentas de la ciudadanía cuando han percibido las graves lesiones que les producía el desarrollo." Debate de totalidad del Proyecto de Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal, *op. cit.*, pág. 7584.

[370] LUCAS MURILLO interpretaba este último inciso de forma que entendía incluida la posterior utilización de los datos en ficheros no automatizados siempre que la información personal se encontrara registrada en soportes físicos susceptibles de tratamiento. El autor entendía que sólo se aplicaba, en consecuencia a una clase de ficheros manuales, ya que en la disposición final 2ª de la LORTAD se establecía la posibilidad de extender el ámbito de aplicación a todos los ficheros de carácter convencional,

lo que establecía la Directiva 95/46/CE, pues era más clara en su aplicación a los ficheros manuales. La LORTAD estaba más alineada con la referencia a fichero automatizado que realizaba el Convenio 108, pese a esta apertura al tratamiento no automatizado, que no se daba en el Convenio 108. Se puede decir que, en este sentido, la LORTAD se quedó a medio camino, entre el Convenio 108 y la Directiva 95/46/CE.

Pese a que se optó por esta referencia a un fichero de datos, en la exposición de motivos, se explicaba que fue desde una concepción dinámica del mismo, ya que también se incluyó la definición de tratamiento de datos. Si acudimos a la definición que la ley hacía del tratamiento eran aquellas "operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias" (art. 3.c LORTAD).

En cuanto a la definición de "fichero automatizado" era "todo conjunto organizado de datos de carácter personal que sean objeto de un tratamiento automatizado, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso" (art. 3.b LORTAD). Por tanto, el fichero era un conjunto de datos que eran objeto de tratamiento automatizado. Hay que entender que, cuando el concepto de tratamiento se refería a que podía ser automatizado o no, debía aludir al inciso comentado sobre el ámbito de aplicación, que también alcanzaba al uso no automatizado de datos en soportes físicos susceptibles de tratamiento.

Los datos de carácter personal se definían como "cualquier información concerniente a personas físicas identificadas o identificables" (art. 3.a LORTAD) aunque esta noción se completaba en el Real Decreto 1332/94, que desarrollaba la LORTAD[371].

---

si el Gobierno, previo informe de la AEPD, así lo decidiera. P. LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal)*, Centro de Estudios Constitucionales, Madrid, 1993, pág. 43.

[371] Así establecía que eran "datos de carácter personal: toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable" (art. 1 Real Decreto 1332/94, de 20 de junio, por el que se desarrollan algunos preceptos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal).

Si bien se denomina al responsable: "responsable del fichero", su poder de decisión recae en el tratamiento. De esta forma se conseguía que el poder recayera en el tratamiento automatizado o no, para que fuera coherente con el ámbito de aplicación general.

Los aspectos concretos sobre los que recaía la capacidad de decisión del responsable eran "la finalidad, contenido y uso del tratamiento". Divergía, por tanto, esta parte de la definición de lo estipulado en el Convenio 108 y de lo previsto en la Directiva 95/46/CE.

En la definición no se aludía al reenvío a otras legislaciones para que designaran directa o indirectamente al responsable. Tampoco indicaba si el responsable debía ser el tratador efectivo de los datos o si podía encomendarle a otro esa labor. No se establecía aún la figura del encargado del tratamiento, aunque sí se preveía en su artículo 27 LORTAD y, por lo tanto, sólo para ficheros de titularidad privada, el supuesto de prestaciones de servicios de tratamiento automatizado de datos[372].

2.3. La Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

Con el fin de transponer la regulación contenida en la Directiva 95/46/CE fue necesario que se aprobara la LOPD. Esta norma incorporó importantes cambios con relación a la anterior LORTAD. Uno de estos cambios fue que la LOPD no incluyó exposición de motivos, por lo que carecemos de esta parte tan importante de la ley para poder interpretarla.

El objeto de la LOPD se especifica en su artículo 1 y es garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los

[372] En concreto el artículo 27 LORTAD establecía: "Prestación de servicios de tratamiento automatizado de datos de carácter personal. 1. Quienes, por cuenta de terceros, presten servicios de tratamiento automatizado de datos de carácter personal no podrán aplicar o utilizar los obtenidos con fin distinto al que figure en el contrato de servicios, ni cederlos, ni siquiera para su conservación, a otras personas. 2. Una vez cumplida la prestación contractual, los datos de carácter personal tratados deberán ser destruidos, salvo que medie autorización expresa de aquél por cuenta de quien se prestan tales servicios, porque razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrán almacenar con las debidas condiciones de seguridad por un período de cinco años".

derechos fundamentales de las personas físicas, y, especialmente, de su honor e intimidad personal y familiar. Hay que tener en cuenta que esta ley se aprueba antes de que el Tribunal Constitucional reconozca el carácter autónomo del derecho a la protección de datos. Por tanto, es lógico que este artículo se centre en su carácter de derecho instrumental y en la protección de los derechos de la personalidad. En lo que se refiere al concepto del responsable se establece:

> "Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento"[373] (art. 3.d) LOPD).

Es prácticamente idéntico al que figuraba en la LORTAD. Pero, aunque a primera vista los cambios son casi inapreciables se convirtieron, gracias a la interpretación jurisprudencial, en cuestiones que han revestido de gran complejidad nuestra regulación del responsable. La cuestión más importante es que, en vez de sustituir "responsable del fichero" por "responsable del tratamiento", de forma que se adaptara a lo establecido por la Directiva 95/46/CE, lo que se hizo fue añadir la palabra tratamiento. Esto ha originado, como se verá, la interpretación de que existen dos figuras y no una: el responsable del fichero y el responsable del tratamiento.

En la construcción de la regulación del responsable también hay que tener en cuenta las aportaciones del tardío desarrollo reglamentario de la LOPD que cristalizó en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD). A esta disposición se trasladaron las interpretaciones que, desde que se aprobó la LOPD se habían realizado sobre esta ley, tanto en la jurisprudencia como en el seno de la AEPD[374]. El RLOPD amplía la definición del responsable:

---

[373] El subrayado es de la autora para señalar los cambios con relación a la definición contenida en el artículo 3.d) LORTAD.

[374] En este sentido, MITJANS PERELLÓ advierte del peligro de la petrificación de los criterios de la AEPD y la jurisprudencia que convertirían al RLOPD en una norma esencialmente interpretativa de la LOPD, lo que iría más allá de lo que corresponde a un reglamento ejecutivo. Y es que esto no permitiría la evolución de la interpretación de una legislación que, en el caso de la protección de datos, precisa ser dinámica. E. MITJANS PERELLÓ, "Impacto de la entrada en vigor del reglamento de desarrollo de la LOPD en el ámbito de actuación de la Agencia Catalana de Protección de Datos", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, pág. 1.977.

> "Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados." (art. 5.1.q) RLOPD)[375].

A continuación se procede al análisis de los elementos del concepto respecto a estas dos definiciones. Sin embargo, antes hay que recalcar que el responsable también se configura como parte esencial de la regulación de la LOPD[376], al igual que se destacó en la Directiva 95/46/CE. Incluso habría que decir que en el ordenamiento español aún ha adquirido mayor relevancia. Ello se debe a que el concepto, además de ser clave como criterio de conexión en la aplicación de la LOPD, de permitir la asignación de responsabilidades y configurar el sujeto obligado a cumplir lo establecido en la normativa, es también criterio para determinar si estamos ante ficheros de titularidad pública o privada, lo que conllevará la aplicación de diferentes regulaciones.

2.3.1. El elemento subjetivo

El elemento subjetivo, de acuerdo con lo que establece la LOPD, es la "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo". Además, hay que añadir la matización del RLOPD: "Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados".

Al igual que se comentara respecto a la definición de la Directiva 95/46/CE, debe primarse la asignación de responsabilidades a la organización que se considere responsable, antes que a la persona concreta que pueda actuar dentro de esta organización[377]. Así lo ha entendido la AEPD que, ante cualquier vulneración que se

[375] El subrayado es de la autora para reflejar los cambios introducido en este concepto respecto al concepto previsto en el artículo 3.d) LOPD.

[376] E. DEL PESO NAVARRO, "La figura del responsable del fichero de de carácter personal en la LORTAD", *Informática y derecho: Revista iberoamericana de derecho informático*, *op. cit.*, pág. 258.

[377] Si bien en un inicio se apuntaba a una postura totalmente contraria por parte de la doctrina. Así DEL PESO NAVARRO entendía que la definición de responsable del fichero establecida en el artículo 3.d) LORTAD no se correspondía con el uso de esta figura en la práctica. Así, este autor distinguía en la práctica la figura del titular o propietario del fichero que entendía era, en el caso del sector privado, el empresario, si era un empresario individual o los reprentantes legales de las sociedades. Por otro lado, aludía a los directores de organización que, en función de las líneas marcadas por los titulares, deciden

ocasiona en el seno de una organización, sanciona a esa organización[378]. Otra cuestión es si un empleado pudiera utilizar los datos de los que tiene conocimiento, en su trabajo, para su propio beneficio. En ese caso, se le debería hacer responsable de su actuación, sin perjuicio de que pudieran atribuirse responsabilidades a la organización, si, por ejemplo, no hubiera adoptado las debidas medidas de seguridad establecidas en la normativa.

La inclusión de las entidades que operan sin contar con personalidad jurídica en el concepto, es un ejemplo del ámbito expansivo de la regulación de protección de datos española. Esta es una opción que no estaba prevista en la Directiva 95/46/CE (sin perjuicio de su admisión en el sector público, cuando se mencionaba "servicio o cualquier otro organismo") y que sólo algunas leyes nacionales han introducido en sus definiciones

---

sobre el tratamiento de los datos. Por último, el autor se refería a los directores informáticos que llevaban a cabo los aspectos técnicos de acuerdo con las instrucciones de los directores de organización. La referencia al titular como figura diferenciada la apoyaba el autor en el artículo 10 LORTAD que aludía al titular del fichero (mención que se ha mantenido en el vigente artículo 10 LOPD) y que lo diferencia del responsable del fichero y en el artículo 3.2 Estatuto de la Agencia de Protección de Datos que, entre las funciones de la misma indicaba la posibilidad de "dirigirse directamente a los titulares y responsables de cualesquiera ficheros de datos de carácter personal". Para el autor la definición del artículo 3.d) LORTAD de responsable del fichero no era la más acertada y constituía un híbrido de las tres figuras apuntadas, según argumentaba con la regulación sobre la figura que se encontraba a lo largo de la LORTAD. En esta regulación se encontraban alusiones a las funciones decisionales (en la definición del artículo 3.d) LORTAD y en el artículo 34 relativa a la formalización de códigos de conducta), a las funciones técnico-organizativas (las relativas a la seguridad de los datos, artículo 9 LORTAD) y a las funciones de gestión (las relativas a los derechos de rectificación y cancelación, artículo 15 LORTAD, a la comunicación de la cesión de datos, artículo 25 LORTAD y a la información a la AEPD, a contrario artículo 36.i) LORTAD). El autor se refería a la inquietud que la LORTAD había causado en los ejecutivos de las empresas porque, pese a que la definición del artículo 3.d) LORTAD se refiriera a personas jurídicas como responsables del fichero, "prácticamente nadie tiene en cuenta esa posibilidad y ve la figura del responsable del fichero con nombre y apellidos propios". Por tanto, el autor ya vaticinaba que la ambigüedad de la definición crearía grandes problemas al aplicarse. E. DEL PESO NAVARRO, "La figura del responsable del fichero de datos de carácter personal en la LORTAD", *Informática y derecho: Revista iberoamericana de derecho informático*, Nº 6-7, 1994, *op. cit.*, págs. 258 a 261 y E. DEL PESO NAVARRO, M.A. RAMOS GONZÁLEZ, *Lortad: análisis de la ley, op.cit.*, págs. 103 a 114. Sin embargo, el mismo autor, al referirse ya a la LOPD, indica que se podría haber aprovechado para suprimir la figura del titular del fichero que contempla el artículo 10 LOPD. E. DEL PESO NAVARRO, *Ley de Protección de Datos: la nueva LORTAD*, Díaz de Santos, Madrid, 2000, págs. 114 a 115.

[378] Así se puede ver al consultar las resoluciones en procedimientos sancionadores que publica la AEPD en su web www.agpd.es y así lo recordó la AEPD que ante la pregunta de cómo se dilucidaba la responsabilidad de empresa y empleado ante un incumplimiento por parte del empleado respecto a las medidas de seguridad indicó que la responsabilidad final no recae sobre la persona física sino sobre el responsable. Por ello, recalcó la AEPD que es esencial realizar un esfuerzo por formar y concienciar al personal. Además, la AEPD citaba como ejemplos algunos casos habituales en los que se produce una vulneración debida a una actuación personal como el caso de incumplimiento del deber de secreto cuando aparecía documentación tirada en la vía pública o cuando aparecían archivos con datos personales que se compartían en redes P2P, cuando se produce un acceso a datos de salud por personas no habilitadas, cuando se produce una contratación fraudulenta (se citaba la SAN de 25 de abril de 2007) o cuando se proporciona información al ex cónyuge. FAQ's 1ª sesión abierta de la AEPD de 22 de abril de 2008, Creación e inscripción de ficheros, Transferencias internacionales, Códigos tipo, Medidas de seguridad, Inspección y potestad sancionadora, pág. 47. http://www.agpd.es/portalwebAGPD/jornadas/1_sesion_abierta/common/faqs_bloque_2.pdf (fecha consulta: 14.2.2015).

de responsable[379]. Así, con este inciso se admite que puedan ser responsables, en virtud de determinadas funciones jurídicas que se les asignan, entidades como pueden ser las sociedades civiles, las comunidades de propietarios, las sucursales o las uniones temporales de empresas[380].

a. Sector público y sector privado

En la Directiva 95/46/CE y en el Convenio 108 la relación de posibles responsables en el sector público incluye los términos autoridad pública, servicio y organismo[381]. La relación establecida en la LOPD se limita a incluir, por un lado, aquellas entidades que se consideren personas, sean de naturaleza pública o privada y, por el otro, añade órgano administrativo, al entender que se trata así de extender la responsabilidad a entidades que no tienen personalidad definida dentro de la administración[382]. Así, se persigue la adaptación a la organización de la administración pública.

Sin embargo, el hecho de no acotarse la definición de responsable, en el sector público, a la organización que ostente personalidad jurídica, aunque es necesario, añade aún más dificultad a la identificación del mismo[383]. El proceso de análisis que conlleva la identificación del fichero, cuando debe cumplirse con la obligación de adoptar la disposición general prevista en la normativa, será primordial en la determinación de quién

[379] En este sentido, en el proyecto del RLOPD de 30 de abril de 2007 se había optado por una solución completamente diferente para este tipo de entidades, de forma que la responsabilidad se atribuía a la persona o personas integrantes de los entes sin personalidad jurídica que decidieran sobre la finalidad, contenido y uso del tratamiento (Art. 5.1.q) del proyecto de Real Decreto por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal, versión de 20 de abril de 2007, publicado por el Ministerio de Justicia).

[380] Estas últimas las menciona S. FARRÉ TOUS, "El encargado del tratamiento en el ámbito de las administraciones públicas", A. TRONCOSO REIGADA, A. (Dir.). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, págs. 1.116 a 1.117.

[381] Las definiciones, tanto de la Directiva 95/46/CE, como del Convenio 108, se encuentran en ambos textos enunciadas en el artículo 2.d).

[382] La única modificación que se realizó en la definición de la LOPD con relación a la definición de la LORTAD respondió a corregir un error del legislador que había incluido la conjunción copulativa "y órgano administrativo" en lugar de la conjunción disyuntiva "u órgano administrativo". Al incluir la conjunción copulativa "y" se acumulaba a los anteriores, de forma que, además, de ser una persona física o jurídica, se añadía el requisito de que fuera órgano administrativo, lo que no tenía sentido, especialmente con relación a la persona física o jurídica de naturaleza privada.

[383] Como recuerda TRONCOSO REIGADA, existe una personalidad jurídica para cada Administración – General del Estado, Autonómica, Local, Corporación de Derecho Público, Universidad- ex artículo 3.4 Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. (BOE núm. 285, de 27.11.1992), que establece que "Cada una de las administraciones públicas actúa para el cumplimiento de sus fines con personalidad jurídica". A. TRONCOSO REIGADA, *La protección de datos personales. En busca del equilibrio, op. cit.*, pág. 304.

debe calificarse como responsable[384]. Aunque hay que tener en cuenta que el órgano que emitirá la disposición general no tiene porque ser el responsable, por lo que, el proceso de reflexión deberá realizarlo este órgano que es, en definitiva, el que atribuirá la responsabilidad[385].

Así, el elemento subjetivo y el fichero aparecen intrínsecamente relacionados en la regulación española, que ha mantenido una doble regulación para ficheros de titularidad pública y ficheros de titularidad privada. Y es que el factor determinante para identificar si estamos en uno u otro tipo de fichero es la titularidad del mismo.

La distinción entre los dos tipos de ficheros ha suscitado, en ocasiones, no pocas dudas. Para intentar solventar estas dudas, en el RLOPD se introdujeron definiciones de ambos tipos de ficheros:

> "Ficheros de titularidad privada: los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica." (art. 5.1.l) RLOPD).
> "Ficheros de titularidad pública: los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público." (art. 5.1.m) RLOPD).

Se plasman en estas definiciones los criterios que había establecido la AEPD para distinguir ambos tipos de ficheros[386]. Estos criterios, principalmente, habían respondido a dos cuestiones. La primera era si el hecho de que una administración pública tuviera cierta participación en una sociedad privada hacía que los ficheros que trataba esta sociedad fueran de titularidad pública o debía estarse a la naturaleza privada de la sociedad y, por tanto, estos ficheros eran de titularidad privada. La segunda cuestión había sido la titularidad de los ficheros que trataban las corporaciones de derecho público.

[384] Ver Capítulo VI.
[385] A. TRONCOSO REIGADA, *La protección de datos personales. En busca del equilibrio, op. cit.*, pág. 304.
[386] Informes de la AEPD de 1999 sobre la naturaleza de los ficheros de responsabilidad de las cámaras de comercio y de 2002 sobre la naturaleza de los ficheros colegiados (ambos sin número de referencia).

La primera cuestión se resuelve, al indicarse que, independientemente de quien ostente la titularidad del capital o de la procedencia de sus recursos económicos, si se trata de una persona, empresa o entidad de derecho privado, debe considerarse que el fichero que trate este tipo de sujetos es un fichero de titularidad privada.

En lo que se refiere a la segunda cuestión, se precisa que las corporaciones de derecho público tratarán dos tipos de ficheros: ficheros de titularidad pública cuando esos ficheros contengan datos que se traten con el fin de que la corporación ejerza las potestades de derecho público que tenga atribuidas[387] y serán ficheros de titularidad privada cuando estos no se traten para llevar a cabo esas potestades de derecho público[388].

b. La normativa autonómica

El elemento subjetivo es importante para establecer la autoridad de control competente. Y es que en España hay que tener en cuenta también la normativa autonómica en esta materia ya que, en virtud del marco competencial, las comunidades autónomas pueden legislar y así lo reconoce la LOPD[389]. Se han aprobado leyes en tres comunidades autónomas: Madrid, Cataluña y País Vasco. No obstante, la Ley 8/2001, de 13 de julio, de protección de datos de carácter personal en la Comunidad de Madrid fue derogada al suprimirse la Agencia de Protección de Datos de la Comunidad de Madrid, fruto de los ajustes que esta Comunidad llevó a cabo en su organización administrativa, con el fin de hacer frente a la crisis económica[390].

Hay que decir que, inicialmente, el criterio utilizado por las leyes autonómicas para delimitar su ámbito de aplicación fue la distinción entre público y privado, de forma

[387] Como ejemplos se puede citar el desarrollo por los colegios profesionales de abogados de la organización del turno de oficio, la gestión por parte de los colegios de procuradores del sistema de notificaciones, el ejercicio de los colegios de la potestad disciplinaria o la gestión del recurso cameral permanente por las cámaras de comercio.

[388] Un ejemplo de estos ficheros sería la gestión del personal de la corporación que se realizará de acuerdo con el derecho laboral.

[389] El artículo 41 LOPD establecía que las autoridades de control autonómicas podrían ejercer sus competencias cuando afectaran a "ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial".

[390] La eliminación de la Agencia se produjo mediante la Ley 8/2012, de 28 de diciembre, de medidas fiscales y administrativas que restituyó las competencias en la materia a la AEPD y derogó la normativa de protección de datos de la Comunidad de Madrid (art. 61 y Disposición derogatoria única), BOCM 29 de diciembre de 2012.

que las mismas limitaban su aplicación a los ficheros de titularidad pública[391]. No obstante, la aprobación del Estatuto de Cataluña modificó este criterio.

i. Cataluña

La Ley 32/2010, de 1 de octubre, de la *Autoritat Catalana de Protecció de Dades* (Ley catalana) derogó la anterior norma[392], fundamentalmente para adaptarse a la regulación establecida en el Estatuto de autonomía catalán de 2006, que amplió el ámbito de actuación de la agencia[393]. Y es que el Estatuto de autonomía catalán extraía del artículo 41 LOPD, que indicaba ficheros "creados o gestionados por las Comunidades autónomas", el máximo partido[394].

A este nuevo ámbito de aplicación había que sumar la adopción por el RLOPD de las nuevas definiciones de ficheros que optaron, en general, por un criterio formal, en vez del criterio material que hasta ese momento había aplicado la *Autoritat Catalana de Protecció de Dades* (ACPD). Es decir, el RLOPD atiende principalmente a la forma jurídica de la entidad que trata los datos para establecer si estamos ante un fichero de titularidad pública o privada. Se excepcionan las corporaciones de derecho público,

[391] A. TRONCOSO REIGADA, "La huida de la administración pública hacia el Derecho Privado y la privatización de los servicios públicos: consecuencias en el régimen jurídico de los ficheros de datos personales y en la delimitación del responsable y del encargado del tratamiento." *Anuario de la Facultad de Derecho de Alcalá de Henares*, nº 2, 2009, págs. 35 a 36.

[392] La norma anterior era la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos.

[393] La aprobación del Estatuto supone el reconocimiento del derecho a la protección de datos que se incluye en el artículo 31, en el apartado, de "*Dels Drets, Deures i Principis Rectors*", en el Capítulo II "*Drets en l'àmbit polític i de l'Administració*". Así esta disposición establece que "todas las personas tienen derecho a la protección de los datos personales contenidos en los ficheros que son competencia de la Generalitat y tienen derecho a acceder a los mismos, examinarlos y rectificarlos. Una autoridad independiente, designada por el Parlamento, ha de velar para que estos derechos sean respetados, en los términos que establecen las leyes."

[394] El artículo 156 del Estatuto de autonomía de Cataluña, que se incluye en el Título dedicado a las competencias, describe las materias sobre las que tendrá competencia la Generalitat en este tema. La competencia será ejecutiva y se extenderá a la inscripción y control de los ficheros o tratamientos de datos creados o gestionados por las instituciones públicas de Cataluña, la Administración de la Generalitat, las administraciones locales, las entidades autónomas y otras entidades de derecho público o privado que dependan de las administraciones autonómica o locales o que presten servicios o que lleven a cabo actividades por cuenta propia a través de cualquier forma de gestión directa o indirecta, además de las universidades catalanas. También se refiere a la inscripción y control de los ficheros o tratamientos de datos privados creados o gestionados por personas físicas o jurídicas para el ejercicio de las funciones públicas con relación a las materias que son competencia de la Generalitat o de los entes locales de Cataluña si ese tratamiento se efectúa en Cataluña. Por último, también, tendrá competencias sobre la inscripción y control de los ficheros o tratamientos de datos creados o gestionados por las corporaciones de derecho público que ejercen sus funciones exclusivamente en el territorio de Cataluña. Será la *Autoritat Catalana de Protecció de Dades* la institución competente para garantizar la protección de los datos en el ámbito de estas competencias.

respecto a las que el criterio adoptado para saber si estamos ante un fichero de titularidad pública o privada es el de si las potestades ejercidas son públicas o no. Hasta la aprobación del RLOPD, la ACPD utilizaba un criterio material, de manera que entendía que el fichero era público si era necesario para el ejercicio de funciones públicas[395].

En definitiva, la Ley catalana se aplica, además de a ficheros y tratamientos que claramente son de titularidad pública[396], a ficheros de entidades privadas en las que ostenten alguna participación importante los entes públicos de la administración catalana, que, de acuerdo con lo previsto en el RLOPD, son ficheros de titularidad privada[397].

Con la ley anterior, la ACPD también tenía competencia cuando estas entidades actuaban por cuenta de las administraciones públicas, como encargadas de tratamiento, lo que se mantiene evidentemente en la Ley catalana de 2010[398].

Por otro lado, con relación a las corporaciones de derecho público, la Ley catalana se centra en el criterio territorial para extender la competencia a todos los ficheros de la entidad, independientemente de que se refieran a potestades públicas o no[399]. También

[395] Esto supuso para la autoridad catalana que se tuviesen que cambiar las notificaciones de algunos ficheros que pasaron de ser públicos a ser privados. E. MITJANS PERELLÓ, "Impacto de la entrada en vigor del reglamento de desarrollo de la LOPD en el ámbito de actuación de la Agencia Catalana de Protección de Datos", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, *op. cit.*, pág. 1.980.

[396] Así, en virtud del artículo 3, apartados a) a d) el ámbito de aplicación de la Ley catalana se refiere a los ficheros y tratamientos de las instituciones públicas, la Administración de la Generalidad, los entes locales, las entidades autónomas, los consorcios y las demás entidades de derecho público vinculadas a la Administración de la Generalidad o a los entes locales, o que dependen de ellos.

[397] De esta forma, en el artículo 3.e) de la Ley catalana se establece que el ámbito de la actuación de la *Autoritat Catalana de Protecció de Dades* comprende los ficheros y los tratamientos que llevan a cabo: "Las entidades de derecho privado que cumplan, como mínimo, uno de los tres requisitos siguientes con relación a la Generalidad, a los entes locales o a los entes que dependen de ellos: Primero. Que su capital pertenezca mayoritariamente a dichos entes públicos. Segundo. Que sus ingresos presupuestarios provengan mayoritariamente de dichos entes públicos. Tercero. Que en sus órganos directivos los miembros designados por dichos entes públicos sean mayoría."

[398] El artículo 3, en sus apartados f) y g) de la Ley catalana, comprende dentro de su ámbito de aplicación "Las demás entidades de derecho privado que prestan servicios públicos mediante cualquier forma de gestión directa o indirecta, si se trata de ficheros y tratamientos vinculados a la prestación de dichos servicios" y "Las personas físicas o jurídicas que cumplen funciones públicas con relación a materias que son competencia de la Generalidad o de los entes locales, si se trata de ficheros o tratamientos destinados al ejercicio de dichas funciones y el tratamiento se lleva a cabo en Cataluña." Estas entidades en principio, parecen susceptibles de encajar en el papel de encargado del tratamiento, aunque, como se verá, habría que analizar caso por caso.

[399] El artículo 3.i) de la Ley catalana comprende así dentro de su ámbito de aplicación "los ficheros y los tratamientos que llevan a cabo las corporaciones de derecho público que cumplen sus funciones exclusivamente en el ámbito territorial de Cataluña a los efectos de lo establecido por la presente ley".

hay que indicar que se aclara la competencia sobre las universidades, independientemente de que sean públicas o privadas[400].

En consecuencia, la Ley catalana establece la posibilidad de sancionar a responsables de los ficheros y de los tratamientos y encargados del tratamiento, cuando las infracciones se cometieran con relación a ficheros de titularidad privada. Para ello, se ha previsto que las sanciones se impongan de acuerdo con lo establecido en la LOPD[401].

ii. País Vasco

La Ley 2/2004, de 25 de febrero de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos (Ley vasca), enuncia en su artículo 2 las entidades que quedan bajo el ámbito de aplicación de la misma[402]. En esta disposición se realiza la enumeración de forma más concreta que en la Ley catalana y, además, se limita claramente a los ficheros creados o gestionados para el ejercicio de potestades de derecho público.

Con relación a esta norma hay que destacar que, a diferencia de la Ley catalana, ha incluido en su texto una regulación sustantiva que es similar a la de la LOPD[403]. Se ha incluido, por lo tanto, una definición de responsable:

También se deja claro en la Guía básica de protección de datos para los colegios profesionales, Generalitat de Catalunya, *Autoritat Catalana de Protecció de Dades*, 2014, pág. 51

[400] El artículo 3 en su apartado h) de la Ley catalana incluye dentro de su ámbito de aplicación "Las universidades públicas y privadas que integran el sistema universitario catalán, y los entes que de ellas dependen."

[401] Así el artículo 21 Ley catalana establece la remisión a la legislación estatal de protección de datos para aplicar el régimen sancionador establecido en la misma y especifica en su apartado 2 que, en caso de infracciones cometidas con relación a ficheros de titularidad privada la resolución que declara la infracción debe imponer las sanciones previstas por la legislación estatal.

[402] El artículo 2 establece concretamente en su apartado 1 que "La presente ley será aplicable a los ficheros de datos de carácter personal creados o gestionados, para el ejercicio de potestades de derecho público, por: a) La Administración General de la Comunidad Autónoma, los órganos forales de los territorios históricos y las administraciones locales del ámbito territorial de la Comunidad Autónoma del País Vasco, así como los entes públicos de cualquier tipo, dependientes o vinculados a las respectivas administraciones públicas, en tanto que los mismos hayan sido creados para el ejercicio de potestades de derecho público. b) El Parlamento Vasco. c) El Tribunal Vasco de Cuentas Públicas. d) El Ararteko.) El Consejo de Relaciones Laborales. f) El Consejo Económico y Social. g) El Consejo Superior de Cooperativas. h) La Agencia Vasca de Protección de Datos. i) La Comisión Arbitral. j) Las corporaciones de derecho público, representativas de intereses económicos y profesionales, de la Comunidad Autónoma del País Vasco. k) Cualesquiera otros organismos o instituciones, con o sin personalidad jurídica, creados por ley del Parlamento Vasco, salvo que ésta disponga lo contrario." (art. 2.1 Ley vasca).

[403] La Ley catalana considera una función de la *Autoritat Catalana de Protecció de Dades* el velar por el cumplimiento de la legislación vigente sobre protección de datos de carácter personal, por lo que se

> "Responsable del fichero o tratamiento: persona, institución, entidad, corporación u órgano administrativo al que está adscrito el fichero y que decide sobre la finalidad, contenido y uso del tratamiento. La disposición por la que se cree el fichero determinará el responsable del mismo. Sus funciones serán las establecidas en el documento de seguridad" (art. 3.d) Ley vasca).

Al establecer esta regulación específica se corre el peligro de originar, una vez más, divergencias en cuestiones que no deberían originarlas, como es la determinación del responsable. Esta definición es un buen ejemplo. Si se atiende a la literalidad del concepto la determinación del responsable vendría por tres aspectos: que tenga adscrito el fichero, que decida sobre la finalidad, contenido y uso del tratamiento y que la disposición que cree el fichero lo determine como tal.

Por lo tanto, tendríamos los clásicos elementos objetivo y funcional que figuran en la LOPD: el poder de decisión sobre la finalidad, contenido y uso del tratamiento. Pero tendríamos dos nuevos elementos que no están en la regulación estatal: la adscripción del fichero y la estipulación en la disposición de creación. Para que esta definición esté de acuerdo con la regulación estatal hay que entender que estos aspectos realmente no deben ser determinantes. En caso contrario, esto podría implicar que para poder considerar a un organismo responsable deberían concurrir los tres elementos, lo que podría llevar a que, si faltara alguno de ellos, no podríamos asignarle responsabilidad. Como ya se ha podido analizar anteriormente, esta postura iría en contra de la finalidad de la creación de la figura del responsable que pretende precisamente todo lo contrario: poder asignar la responsabilidad al sujeto que decide *de facto* sobre el tratamiento.

2.3.2. El elemento objetivo

Si bien el elemento objetivo de la definición se centra en el "tratamiento", sin aludir ni a los datos personales ni al fichero, es preciso realizar una revisión de todos estos conceptos. El tratamiento se define como "tratamiento de datos", por lo que ya incluye a los datos como parte intrínseca del concepto (art. 3.c) LOPD). Asimismo, el responsable se designa como "responsable del fichero o tratamiento", por lo que se pone de manifiesto la importancia que el fichero también desempeñará en la configuración de

---

entiende que debe aplicar la LOPD, al carecer esta ley de una regulación sustantiva del derecho de protección de datos (art. 5.a Ley catalana).

la figura del responsable. A esto hay que añadir que el ámbito de aplicación de la LOPD se define como: "aquellos datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado" (art. 2.1 LOPD).

a. Datos de carácter personal

La LOPD recoge como definición de dato personal la primera parte de la definición de la Directiva 95/46/CE, es decir, "cualquier información concerniente a personas físicas identificadas o identificables" (art.3.a) LOPD), ya que no se modificó del texto de la LORTAD. La LORTAD optó por complementar esta definición con la de "procedimiento de disociación", que es "todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable", lo que fue mantenido por la LOPD (art. 3.f LOPD)[404]. Por tanto, no había definición ni orientación de lo que podía entenderse que era persona identificada o identificable.

Sin embargo, en línea con lo indicado por el GA29, la AEPD también ha entendido que para que el uso de datos disociados excluya la aplicación de la legislación de protección de datos debe ser una disociación irreversible, de forma que se asegure el anonimato de las personas[405]. Esta interpretación se confirmó en el RLOPD que reformuló la definición. Se añadió una definición de "dato disociado: aquél que no permite la identificación de un afectado o interesado" (art. 5.1.e) RLOPD) y se completó

[404] Llama la atención que se establezca una definición específica para este procedimiento de disociación cuando en la ley sólo se alude a él una vez en el artículo 11.6 LOPD donde se establece la regulación de la cesión de datos, que especifica que no se aplicará lo establecido en el artículo 11 LOPD si la comunicación se efectúa previo procedimiento de disociación. Por lo tanto, la utilización de este procedimiento en principio parece que sólo eximiría de aplicar la regulación de la comunicación de datos. Aunque debe entenderse que si el procedimiento de disociación garantiza que la persona no sea identificable, el tratamiento de estos datos no debería entrar en el ámbito de aplicación de la LOPD. Así lo ha entendido la AEPD, Informe 37/2010 de la AEPD, pág. 1.

[405] Así ha sido interpretado por la AEPD que para que no se aplique la legislación de protección de datos exige que "De este modo para que un procedimiento de disociación pueda ser considerado a los efectos de la Ley Orgánica 15/1999, será necesario que de la aplicación de dicho procedimiento resulte imposible asociar el dato o datos de que se disponga a un sujeto determinado. Esta Agencia ha venido señalando que para ello será preciso que no exista la posibilidad, incluso remota, de que, mediante la utilización, con carácter previo, coetáneo o posterior de cualquier medio (proceso informático, programa, herramienta del sistema, etc.), la información concerniente a los afectados por el tratamiento de datos, que obre en poder del consultante, pueda revelar su identidad." Informe 352/2011 de la AEPD, pág. 3. Para ver postura del GA29 ver Capítulo II.

con una definición más de "procedimiento de disociación: todo tratamiento de datos personales que permita la obtención de datos disociados" (art. 5.1.p) RLOPD)[406].

Con el objetivo de incluir de forma más completa la regulación que se hallaba en la Directiva 95/46/CE, el RLOPD amplió la definición de datos personales, añadió una definición de persona identificable y también una de datos de salud:

> "Dato de carácter personal: cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables" (art. 5.1.f) RLOPD).
> "Persona identificable: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultura o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados." (art. 5.1.o) RLOPD)[407].
> "Datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética" (art. 5.1.g) RLOPD).

[406] En el RLOPD no abundan tampoco las referencias a este procedimiento de disociación. Se utiliza en el artículo 8.6 RLOPD que versa sobre el principio de calidad, de forma que establece que para poder conservar datos personales una vez ya se ha cumplido el período en el que puede exigirse algún tipo de responsabilidad, sólo podrán ser conservados previa disociación de los mismos. También se alude a este procedimiento en el artículo 116.4 RLOPD para referirse a la publicación de las resoluciones de los procedimientos que tramita la AEPD, de forma que debe realizarse previa disociación de los datos que se incluyen en ellas.

[407] La AEPD, en su Informe 0654/2009, responde a una consulta en la que se plantea si resulta aplicable la LOPD a un fichero cuyo objetivo es llevar a cabo un proyecto de investigación y que contiene datos relativos a reacciones alérgicas, test y datos relativos al paciente a quien se identifica con un código numérico. Este informe remite, a su vez, a otro anterior, de 22 de septiembre de 2008, en el que la AEPD indicaba que debían tenerse en cuenta en este contexto médico las definiciones previstas en la Ley 14/2007, de 3 de julio, de investigación biomédica que delimitaban los supuestos en los que debía aplicarse la legislación de protección de datos. De esta forma, esta ley es un ejemplo de cómo una ley aplicable a un sector concreto especifica una regulación en materia de protección de datos. Así, esta norma incluye en su apartado de definiciones, letras p) a r), los siguientes conceptos: "Muestra biológica anonimizada o irreversiblemente disociada: muestra que no puede asociarse a una persona identificada o identificable por haberse destruido el nexo con toda información que identifique al sujeto, o porque dicha asociación exige un esfuerzo no razonable. Muestra biológica no identificable o anónima: muestra recogida sin un nexo con una persona identificada o identificable de la que, consiguientemente, no se conoce la procedencia y es imposible trazar el origen. Muestra biológica codificada o reversiblemente disociada: muestra no asociada a una persona identificada o identificable por haberse sustituido o desligado la información que identifica a esa persona utilizando un código que permita la operación inversa." Como indica la AEPD en su informe mientras las dos primeras categorías quedarían excluidos del ámbito de aplicación de la LOPD, en la tercera sí que debería aplicarse esta ley.

De esta forma, hay datos que, si bien no identificarán de forma directa al interesado, podrán ser considerados datos de carácter personal, porque facilitan, sin esfuerzos desproporcionados, la identificación del mismo[408].

b. Fichero y tratamiento

Con el fin de adaptar la regulación a la Directiva 95/46/CE se tuvo que ampliar el ámbito de aplicación, no sólo a los ficheros automatizados, a los que se aplicaba claramente la LORTAD, sino también a los ficheros no automatizados, a los que sólo se aplicaba en parte. Por eso, se eliminó de la definición de fichero de la LORTAD la palabra "tratamiento", de forma que así la noción se adaptaba mejor a todo tipo de soportes: "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso" (art. 3.b LOPD). El RLOPD estableció su propia definición de fichero y añadió una de fichero no automatizado:

> "Fichero: todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso." (art. 5.1.k) RLOPD).
> "Fichero no automatizado: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica".(art. 5.1.n) RLOPD).

La principal aportación de ambas definiciones era la necesidad de que el fichero permitiera el acceso con arreglo a criterios "determinados", en el caso del fichero y "específicos relativos a personas físicas", en el caso del fichero no automatizado[409]. Este último además debe ser estructurado y podrá localizarse en diferentes ubicaciones.

---

[408] En el Informe 0427/2010 la AEPD indica que datos como el número de identificación fiscal, el documento nacional de identidad o el número de matrícula de un vehículo ya suponen por sí solos un tratamiento de datos personales. De esta forma, la AEPD sigue la interpretación que el GA29 realiza sobre los datos conocidos como "identificadores" y que se menciona en el Capítulo II. En este sentido, también hay que mencionar su controvertida interpretación sobre el carácter de dato personal de la dirección IP. Informe 327/2003 AEPD. Ver J.L. PIÑAR MAÑAS, "Concepto de dato personal", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, págs. 206 a 213.

[409] Como afirma PALOMAR OLMEDA, lo esencial en estas definiciones es que, con independencia del método y de la tecnología utilizada, exista un sistema de búsquedas. PALOMAR OLMEDA, A., "Obligaciones previas al tratamiento de datos", MARTÍNEZ MARTÍNEZ, R. (Coord.), VVAA, *Protección de datos: comentarios a la LOPD y su reglamento de desarrollo*, Tirant lo Blanch, Valencia, 2009, pág. 64.

En sintonía con lo establecido por la Directiva 95/46/CE, se pretende restringir así la aplicación de la normativa a los ficheros no automatizados, en virtud del sistema de acceso a los datos. No obstante, hay que recordar que la Directiva 95/46/CE, lo que hace es utilizar el concepto de fichero para limitar su aplicación a ficheros manuales, de forma que exige que revista la forma de conjunto estructurado de datos, accesibles con arreglo a criterios determinados, que debían determinar los Estados miembros. No existe en la Directiva 95/46/CE el concepto de fichero automatizado, sino que se centra en el tratamiento. Y es que los sistemas automatizados permiten naturalmente cumplir con estos requisitos de organización y acceso.

La AEPD ha interpretado una noción amplia de fichero no automatizado[410]. Esta interpretación fue rechazada por el Tribunal Supremo en el polémico caso de los Libros bautismales, ya que el Alto tribunal consideró que estos libros, ordenados por fecha de bautismo, no podían considerarse organizados de acuerdo con criterios relativos a personas físicas[411].

[410] Mediante el Informe 0279/2009, la AEPD respondía a una consulta relativa a la existencia o no de fichero cuando en una carpeta en soporte papel, la documentación se encuentra ordenada según las fechas de creación de los documentos incorporados. La AEPD entendió que la ordenación de estos documentos por fecha no cumpliría, en principio, con el requisito de que los criterios fueran relativos a personas físicas. Ahora bien, la AEPD puntualizaba que se debía asegurar que esta ordenación no permitía el acceso a los datos personales, sin esfuerzos desproporcionados. Si existiera una correlación entre las fechas de los documentos y las personas físicas que implicara que se pudiera acceder a los datos de éstas sin esfuerzos desproporcionados, obligaría a considerar que la carpeta consituiría un fichero no automatizado. En el mismo informe y en alusión a los ficheros automatizados, la AEPD recalca que todo sistema informático lleva aparejada una organización, ya que todo sistema informático permite hacer búsquedas de documentos, lo que implica que en el caso que se plantea en la consulta de documentos electrónicos incorporados, sin ningún orden lógico en un soporte, constituye un fichero.

[411] Respecto al asunto de los libros de bautismo, la AEPD había considerado que estos registros que mantiene la Iglesia católica en soporte no automatizado debían considerarse ficheros y, por tanto, les era aplicable la legislación de protección de datos. Sin embargo el Tribunal Supremo consideró que los libros "son una pura acumulación de estos (datos) que comporta una difícil búsqueda, acceso e identificación en cuanto no están ordenados ni alfabéticamente, ni por fecha de nacimiento, sino sólo por las fechas de bautismo, siendo absolutamente necesario el conocimiento previo de la Parroquia donde aquel tuvo lugar, no resultando además accesibles para terceros distintos del bautizado, que no podrían solicitar ajenas partidas de bautismo" STS de 19 de septiembre de 2008 (Sala 3ª) (ROJ: STS 4646/2008) FJ 4º. Hay que tener en cuenta que, según la nota de prensa de la AEPD cuando se emitió la sentencia, desde el año 2006 hasta el 2008 se habían presentado ante la AEPD unas 650 solicitudes de ejercicio del derecho de cancelación de los datos de estos libros, solicitudes que habían presentado apóstatas que no querían que constaran sus datos en estos registros. Nota de prensa de la AEPD de 30.9.2008.: http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2008/notas_prensa/common/sept/np_080930_sentencia_TS.pdf, (fecha consulta: 10.2.2015).

El tratamiento se define en la LOPD y en el RLOPD (art. 5.1.t), aunque en éste las diferencias respecto al de la LOPD no son muy relevantes, al añadir sólo algunas operaciones a la enumeración realizada[412]:

> "Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias" (art. 3.c) LOPD).

En la LOPD, a diferencia de la LORTAD, el fichero ya no es un conjunto organizado de datos objeto de tratamiento, sino sólo un conjunto organizado de datos. El responsable, pese a que en su denominación incluye que es responsable del fichero o del tratamiento, se define como la persona que decide sobre la finalidad, contenido y uso del tratamiento. Por tanto, lo que define al responsable es esta capacidad de decidir sobre el tratamiento, quedando el fichero fuera del elemento objetivo. En coherencia con este hecho carecería de sentido hablar de responsable del fichero, ya que lo verdaderamente esencial para determinar si el responsable es tal, es su capacidad de decidir sobre el tratamiento.

Una forma de mantener la conexión entre tratamiento y fichero y, por tanto, de preservar la utilidad del concepto de fichero en la regulación, sería seguir la interpretación apuntada por la AEPD, a raíz de una sentencia de la Audiencia Nacional[413]. Según esta interpretación, para que un tratamiento quedara dentro del ámbito de aplicación de la normativa de protección de datos debería enmarcarse en un fichero, por lo que, sin fichero no habría tratamiento de datos[414]. De hecho, esta interpretación respecto a los ficheros no automatizados estaría de acuerdo con la Directiva 95/46/CE.

[412] Concretamente se añaden las operaciones relativas a la consulta, utilización y supresión.
[413] SAN de 16 de febrero de 2006 (Sala de lo contencioso-administrativo) (ROJ: SAN 822/2006).
[414] La AEPD remite a la SAN de 16 de febrero de 2006 (Sala de lo contencioso-administrativo) (ROJ: SAN 822/2006), que se refiere al tratamiento de datos personales y relaciona este concepto con el de fichero, al que configura como un *prius* necesario para la aplicación de la Ley Orgánica 15/1999, razona, así, la sentencia: "Pues bien, para que una actuación manual sobre datos personales (recogida, grabación, conservación, elaboración, modificación, bloqueo...) tenga la consideración de "tratamiento de datos personales" sujeto al sistema de protección de la Ley Orgánica 15/1999 es necesario que dichos datos estén contenidos o destinados a ser incluidos en un fichero, esto es, en un conjunto estructurado u organizados de datos con arreglo a criterios determinados. Si no es así, el tratamiento manual de datos personales quedará fuera del ámbito de aplicación de la ley, no será un "tratamiento de datos personales" según el concepto normativo que la ley proporciona." Informe 573/2009 de la AEPD.

En este sentido, la Audiencia Nacional señala la diferencia entre la Directiva 95/46/CE y la LOPD en su determinación del ámbito de aplicación[415]. La Directiva 95/46/CE se aplicará al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

En cambio la LOPD establece un ámbito de aplicación más genérico, de forma que será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado. Así, para la Audiencia Nacional queda claro que el registro de los datos en soporte físico equivale a un fichero, de forma que la existencia de este fichero para la normativa española se constituye en un *prius* necesario en caso de ficheros manuales. La Audiencia Nacional añade a este respecto que, en el caso de tratamientos automatizados, siempre sometidos a la ley, es difícil imaginar que no exista fichero[416].

Este criterio no se ha consolidado y queda claro que, en el ámbito, por ejemplo de la videovigilancia se admite que no exista fichero, sino sólo tratamiento de datos cuando no se graban las imágenes, sino que se emiten en tiempo real[417]. Veremos otros supuestos en los que sólo existirá tratamiento, cuando se aborde la figura del responsable del tratamiento frente a la de responsable del fichero.

No obstante y pese a estas consideraciones entorno a la utilidad o no del concepto de fichero, lo que parece claro es que para determinar quien será responsable del fichero o del tratamiento, lo único que debe tenerse en cuenta es el poder de decisión respecto del

[415] SAN de 16 de febrero de 2006 (Sala de lo contencioso-administrativo) (ROJ: SAN 822/2006).
[416] SAN de 16 de febrero de 2006 (Sala de lo contencioso-administrativo) (ROJ: SAN 822/2006), FJ 3. Sin embargo, esta interpretación de la Audiencia Nacional seguida por la AEPD había sido contradicha por la misma agencia en otro informe anterior del mismo año, en el que indicaba que, de acuerdo con lo que establecía el art. 2.1 LOPD, no haría falta esta conexión con un fichero para poder aplicar la normativa. Así, la AEPD en el Informe 0279/2009 indicaba que si se producía un tratamiento de datos con información concerniente a personas físicas identificadas o identificables, de acuerdo con el art. 2.1 LOPD, con independencia de si se crea o no un fichero, se aplicará la LOPD. La AEPD incidía en que lo importante era que los datos pudieran ser tratados.
[417] Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras (BOE núm. 296, 12.12.2006, pág. 43458-43460).

tratamiento, no respecto del fichero, ello sin perjuicio de lo que se comentará sobre la corresponsabilidad.

Sin embargo, la identificación del fichero es un paso previo obligado, ya que el responsable debe notificarlo antes de iniciar el tratamiento[418]. De esta forma, el responsable se verá en la necesidad de determinar todos los elementos que lo integren y que se tendrán en cuenta para cumplir la legislación[419]. La regulación no nos ofrece pautas concretas, respecto al fichero, que ayuden a delimitarlo. La doctrina ha creado, por ello, la noción de fichero jurídico, que se diferenciaría del fichero informático o del fichero físico, de forma que la determinación del mismo se realizaría en virtud de la finalidad para la que se traten los datos personales que contiene[420]. El fichero jurídico sería el que tiene relevancia a efectos de protección de datos. Así, este fichero podrá localizarse en diferentes ubicaciones o integrarse de diversos soportes o sistemas. Y es que los ficheros pueden ser mixtos, es decir que constarán de partes automatizadas y partes no automatizadas[421].

c. Exclusiones del ámbito de aplicación

Al igual que en el análisis de la Directiva 95/46/CE, el estudio del ámbito de aplicación territorial de la LOPD se abordará más adelante[422].

Es necesario para conocer el objeto sobre el que actuará el responsable, aludir a las exclusiones establecidas en la regulación española con relación a los fallecidos, las personas jurídicas, los datos de contacto y los empresarios individuales.

[418] Ver Capítulo VI.
[419] Si tiene algo positivo el trámite de notificación de ficheros es que obliga a realizar esta toma de contacto con la normativa que es este proceso reflexivo sobre la identificación del fichero. Como indica TRONCOSO REIGADA, la notificación de ficheros facilita que el responsable sea consciente de que esa información no le pertenece sino que es de las personas que son dueñas de sus datos. A. TRONCOSO REIGADA, *La protección de datos personales. En busca del equilibrio*, *op. cit.*, pág. 297.
[420] M.A. DAVARA RODRÍGUEZ "El concepto de fichero en la normativa sobre protección de datos", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, *op. cit.*, pág. 219.
[421] Así en el momento de notificar los ficheros debe indicarse en el formulario de notificación si el fichero es automatizado, no automatizado o mixto.
[422] Ver Capítulo IV.

Como ya se indicaba con relación a la Directiva 95/46/CE, los colectivos relativos a fallecidos y personas jurídicas, en principio, no eran objeto de protección en la misma, si bien nada obstaba para que los Estados miembros ampliaran el ámbito de aplicación de sus leyes para incluirlos. La LOPD no hacía referencia explícitamente a esta cuestión pero, al tratarse de un derecho ligado a la personalidad, su protección se atribuyó a las personas físicas y quedaron fuera de su ámbito los fallecidos y las personas jurídicas[423]. No obstante, el RLOPD posibilitó que las personas vinculadas al fallecido pudieran dirigirse a los responsables que trataran datos del fallecido para notificar el óbito y poder solicitar la cancelación de los datos[424].

El RLOPD incluyó otras exclusiones que pretendían facilitar la gestión ordinaria de las empresas. Sin embargo, su incorporación no estuvo exenta de polémica, ya que restringía el ámbito de aplicación de la LOPD y además no quedaba claro cómo aplicarlas en la práctica. La primera exclusión se reproduce a continuación:

> "Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales."(art. 2.2 RLOPD)

Con este precepto se pretendía dejar fuera de la regulación las agendas corporativas, los llamados datos de contacto. Se suscitaron algunas dudas como el significado de "personas físicas que presten sus servicios", ya que parecía apuntar a proveedores en vez de empleados. También se planteó si la lista exhaustiva de los datos que debían considerarse fuera del ámbito de aplicación implicaba que, en caso de tener algún dato adicional de esa persona, no podía aplicarse la exclusión y debían incluirse dentro del ámbito de aplicación todos los datos que se vincularan con esa persona.

[423] Con relación a la exclusión del ámbito de aplicación de la legislación de los datos de fallecidos, lo recuerda la AEPD en su Informe 523/2010 y anteriormente en su Informe 365/2006, en el que advierte que "si bien el derecho a la protección de datos desaparecería como consecuencia de la muerte de las personas, no sucede así con el derecho de determinadas personas para ejercitar acciones en nombre de las personas fallecidas, con el fin de garantizar otros derechos constitucionalmente reconocidos" y cita como ejemplo la LO 1/1982.

[424] Se pretendía evitar el hecho de no poder solicitar la cancelación de datos, por ejemplo, en casos en los que el responsable, al ignorarlo, continúe enviando notificaciones o correspondencia al fallecido. Concretamente el apartado 4 del artículo 2 del RLOPD especifica: "Este reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos."

La AEPD emitió diversos informes en los que indicaba las pautas para aplicar esta previsión[425]. El tratamiento de datos se debía limitar a la lista indicada, ya que eso implicaba la accidentalidad del tratamiento y la finalidad del tratamiento debía ser el contacto con la persona jurídica. Además, no era preciso que estos datos se refirieran sólo a empleados sino que, la amplitud del precepto, permitía incluir también datos de apoderados[426].

Asimismo, el RLOPD excluyó del "régimen de aplicación de la protección de datos de carácter personal" "a los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros" (art. 2.3 RLOPD). La principal cuestión suscitada era qué debía entenderse por "empresarios individuales" y qué quería decir cuando hicieran referencia a ellos "en su calidad de" comerciantes, industriales y navieros. La AEPD interpretó que entrarían en esta definición aquellas personas físicas que hubieran organizado su actividad bajo la forma de empresa[427]. La AEPD mencionaba, como un ejemplo de este supuesto, cuando el nombre comercial o la marca utilizada por el empresario fueran sus datos personales. No obstante, también se establecía una limitación relativa a la finalidad del tratamiento. Sólo se podrían utilizar los datos de este empresario si la finalidad se relacionaba con su condición de empresario[428].

La controversia sobre la extralimitación del RLOPD respecto a estas exclusiones, parece que ha llegado al Tribunal Supremo que, si bien en referencia al orden civil, las

[425] Informes 42/2008, 78/2008, 200/2008 y 234/2008 de la AEPD.
[426] Respecto a los apoderados o representantes de una empresa, la Audiencia Nacional se ha pronunciado en dos sentencias relativas a la denegación del ejercicio del derecho de cancelación. Son asuntos similares en los que una persona, representante de una empresa solicitaba a titulares de páginas web la supresión de informaciones que criticaban la actividad de la empresa y mencionaban al representante. La Audiencia Nacional ha considerado que no procedía la cancelación al considerarse la información relativa a la persona jurídica y aplicarse la exclusión del artículo 2.2 RLOPD. SAN de 16 de julio de 2009 (Sala de lo contencioso-administrativo) (ROJ: SAN 3804/2009) y SAN de 9 de junio de 2011 (Sala de lo contencioso-administrativo) (ROJ: SAN 2846/2011).
[427] La AEPD indicaba que los comerciantes individuales se incluirían dentro del ámbito de aplicación de la LOPD cuando no fuera posible diferenciar su actividad mercantil de la actividad privada. Los profesionales quedarían bajo el ámbito de aplicación de la LOPD si no tuvieran organizada su actividad profesional bajo la forma de empresa y no ostentaran la condición de comerciante, como los profesionales liberales cuyas actividades están expresamente excluidas del ámbito de aplicación de la Ley Básica 3/1993, de 22 de marzo, Básica de las Cámaras Oficiales de Comercio, Industria y Navegación (la AEPD hacía referencia a esta norma que ha sido posteriormente derogada por la Ley 4/2014, de 1 de abril, Básica de las Cámaras Oficiales de Comercio, Industria, Servicios y Navegación). Informe 234/2008 de la AEPD.
[428] Informes 42/2008, 78/2008 y 234/2008 de la AEPD.

cuestiona. Así, el Alto tribunal deja la puerta abierta a entender que esta previsión reglamentaria no puede significar que se excluya del ámbito de aplicación de la normativa reguladora del derecho a la protección de datos a las personas físicas que reúnan la condición de comerciante, cuando no han sido excluidas por la LOPD ni por el resto de normas internacionales que regulan este derecho[429].

También hay que hacer referencia a los ficheros que se entienden excluidos y aquellos que se regularán por su regulación específica y, de forma subsidiaria por la LOPD. Los ficheros a los que no se aplica la LOPD son:

> a) A los mantenidos por personas físicas para el ejercicio de actividades exclusivamente personales o domésticas b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada (art. 2.2 LOPD)

Sin embargo, con relación a los últimos sí se exige que se cumpla con la obligación del responsable de comunicar previamente la existencia del mismo, sus características generales y su finalidad a la AEPD[430].

El RLOPD vuelve a recoger estas exclusiones pero respecto a la primera categoría de ficheros, los mantenidos por personas físicas para el ejercicio de actividades personales o domésticas establece su artículo 4.a) *in fine* que "sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares".

También se incluyen en la LOPD algunos ficheros que se remiten a su regulación especial. No obstante, se añade que si se incluye alguna disposición específica relativa a estos ficheros en la LOPD también se deberá aplicar. Se trata de:

> "a) Los ficheros regulados por la legislación de régimen electoral b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o

[429] El Tribunal Supremo señala concretamente que "un reglamento no puede excluir de la protección de una ley orgánica de desarrollo de un derecho fundamental a quienes la Constitución, el Convenio, la Directiva y la propia ley orgánica no han excluido". STS de 21 de mayo de 2014 (Sala 1ª) (ROJ: STS 267/2014), FJ 7.

[430] Hay que recordar que el artículo 3.1 Directiva 95/46/CE establecía la exclusión de su ámbito de aplicación de aquellos tratamientos de datos efectuados en el ejercicio de actividades fuera de lo que era el primer pilar relativo al derecho comunitario y que eran en todo caso las relativas a la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal. Esto llevó a que en España se entendieran excluidos estos ficheros y, sin embargo, se optó por establecer una regulación parcial para los ficheros de las fuerzas y cuerpos de seguridad, como se indica a continuación.

autonómica sobre la función estadística pública c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del Régimen del personal de las Fuerzas Armadas d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad" (art. 2.3 LOPD).

2.3.3. El elemento funcional

El responsable en la LOPD se determina por su poder de decidir sobre la finalidad, contenido y uso del tratamiento. Para identificar de donde emana el poder de decisión del responsable existen dos fuentes principalmente: la normativa y las circunstancias del supuesto de hecho. A continuación se analizarán estas dos vías de atribución de responsabilidad y el alcance de los aspectos concretos sobre los que se exige que el responsable tenga esta capacidad de decidir. Posteriormente se incidirá en el especial supuesto de corresponsabilidad que contempla la legislación española.

a. El origen de la capacidad de decidir del responsable

i. El poder de decidir emana de una competencia legal

Lo primero que hay que destacar del concepto de responsable de la ley española es que no se ha incluido el reenvío a la legislación para la designación directa o indirecta del responsable, establecido por la Directiva 95/46/CE. Como ya comenté, el reenvío es más bien una indicación al legislador, por lo que no implicaría la imposibilidad de utilizarlo.

Si bien, como señalaba el GA29, lo esencial para determinar el poder de decisión deben ser las circunstancias de hecho, no hay que perder de vista que el responsable está limitado en su actuación por el entorno normativo que regula su actividad. Esto es especialmente patente en el sector público, en el que la identificación del responsable estará fuertemente conectada con la competencia para ejercer las funciones públicas. De hecho, es este ámbito en el que tiene más sentido el reenvío que realizaba la Directiva 95/46/CE, con el fin de respetar la organización de la administración pública de los

Estados miembros[431]. No obstante, los operadores privados en virtud de la actividad que realicen, también pueden verse sometidos a una fuerte regulación.

Lo habitual, cuando tenemos que identificar, en un supuesto de hecho, al responsable es que lo primero que hagamos sea acudir a la normativa que resulta aplicable al sujeto analizado. En esa legislación podríamos encontrar que se designa exactamente quién es este responsable o, lo más usual, es que hallemos una definición de las obligaciones establecidas por esa ley y de los sujetos obligados a cumplirlas. Si el cumplimiento de estas obligaciones conlleva el tratamiento de datos, deberemos analizar si la configuración de las mismas implica que el sujeto obligado tiene la capacidad de decidir sobre la finalidad, contenido y usos del tratamiento derivado de este cumplimiento[432].

Un ejemplo de determinación legal del responsable es la Ley de mediación de seguros y reaseguros privados. En esta ley se establece una sección dedicada a la protección de datos, en la que califica como responsables a los corredores de seguros y como encargados de las compañías a los agentes de seguros[433]. Se trata de un caso en el que el legislador es el que ha realizado el análisis y ha aplicado los conceptos.

En este caso, el legislador no ha dejado margen de maniobra e incluye también una referencia al tratamiento que considerará legitimado de acuerdo con la ley y lo que precisará de consentimiento por parte del cliente[434]. De nuevo, hay que plantear si esta opción de incluir una regulación de protección de datos en una norma sectorial es la más

[431] En este sentido, también hay que recordar el Considerando 32 Directiva 95/46/CE que remite a las legislaciones nacionales para determinar si el responsable del tratamiento que tiene conferida una misión de interés público o inherente al ejercicio del poder público, debe ser una administración pública u otra persona de derecho público o privado, como por ejemplo una asociación profesional.

[432] Como ejemplo se puede citar el Informe de la AEPD 106/2008 que, precisamente, versa sobre una consulta en la que se plantea quién será responsable de los datos clínicos que trata una clínica privada. La AEPD acude a la Ley 41/2002 mencionada, ya que es la que regula la historia clínica. En esta ley identifica que las obligaciones relativas a esta información clínica las debe cumplir el centro sanitario. Especialmente la obligación de custodia se indica que debe estar a cargo de la dirección del centro sanitario. También se indica que, en el caso que los profesionales sanitarios desarrollaran su actividad de forma individual deberían ser responsables de esta custodia y gestión. Sin embargo, en el caso planteado, la AEPD entiende que los facultativos que trabajan en el centro tienen una relación de dependencia con el centro, sea laboral o mercantil, y que los pacientes son del centro y no de los facultativos, por lo que correspondería al centro médico el tratamiento y custodia de las historias clínicas y, por tanto, también debe considerarse, en consecuencia, al centro responsable.

[433] Artículo 62 Ley 26/2006, de 17 de julio, de mediación de seguros y reaseguros (BOE núm. 170 18.7.2006).

[434] Artículo 63 Ley 26/2006.

acertada. La Directiva 95/46/CE le da cabida, ya que además de incluir el reenvío en el concepto de responsable del tratamiento a la legislación para la designación del mismo, también especifica, como posibles opciones legislativas para transponer la Directiva la aprobación de una norma general o introducir la regulación en normas sectoriales[435].

No obstante, si, como indicó el GA29, lo importante es tener en cuenta la capacidad de influencia de hecho y si se tienen en cuenta los complejos modelos de negocio que aparecen en una sociedad tan cambiante como la actual, hay que valorar cuando será oportuno incluir una regulación en una norma sectorial. Lo más importante, en todo caso, sería tener una norma general clara que permita su adaptación a los diferentes sectores, mediante la interpretación de responsables, autoridades, tribunales y afectados. La inclusión de regulaciones de protección de datos en normas sectoriales, si bien tiene la ventaja de clarificar a ese sector cómo debe aplicar esa normativa y además cuenta con la participación de las autoridades de protección de datos, que deben emitir informes al respecto, tiene también el riesgo de crear tensiones entre lo estipulado en la norma y la realidad.

La opción de incluir una regulación en una normativa sectorial sí será adecuada cuando lo que se pretenda es aumentar el nivel de protección del derecho de protección de datos, en virtud del sector en concreto, o cuando en este sector ya haya una tradición de protección de los datos que sea innata al mismo y que puede derivar de otros derechos. Esto sucede, por ejemplo, en el sector sanitario o en el sector de las telecomunicaciones o comunicaciones electrónicas[436].

[435] Así el Considerando 23 Directiva 95/46/CE establece que "Considerando que los Estados miembros están facultados para garantizar la protección de las personas tanto mediante una ley general relativa a la protección de las personas respecto del tratamiento de los datos de carácter personal como mediante leyes sectoriales, como las relativas a los institutos estadísticos".

[436] La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (BOE núm. 114 10.5.2014) incluye el artículo 41 sobre la protección de los datos de carácter personal que además en su apartado 4 remite a lo establecido por la LOPD y en su artículo 48 establece el derecho a la protección de datos personales y la privacidad en relación con las comunicaciones no solicitadas, con los datos de tráfico y de localización y con las guías de abonados. Además el Real Decreto 424/2005, de 15 de abril, por el que se aprueba el reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios (BOE núm. 102 29.4.2005) que desarrollaba la anterior Ley General de Telecomunicaciones incluye también una regulación sobre la protección de los datos personales en el Capítulo I del Título V (artículos 61 siguientes). Respecto al sector sanitario la Ley 33/2011, de 4 de octubre, General de Salud Pública (BOE núm. 240 5.10.2011) establece en su artículo 7 dedicado al derecho a la intimidad, confidencialidad y respeto de la dignidad, que la información personal empleada en las actuaciones de salud pública se regirá por la LOPD y la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (BOE núm. 274 15.11.2002).

Sin embargo, en estas normas no se ha incluido ninguna designación expresa de quién debe ser considerado responsable o encargado[437]. En esta normativa, así como en otra, en la que ni siquiera se realice una mención a la regulación de protección de datos (que, por otro lado, será lo habitual), se pueden encontrar aspectos que ayuden a identificar si se está ante un responsable o ante un encargado[438]. Estos aspectos pueden ser funciones u obligaciones que deba cumplir un sujeto que denoten que este sujeto deberá decidir sobre el tratamiento y que responderían a la competencia implícita a la que aludía el GA29.

Con este análisis de la normativa sectorial se pone a prueba la calidad de la técnica legislativa. De esta forma, si la norma realiza una buena definición de las obligaciones y de los sujetos obligados, será más fácil determinar quien ostenta la capacidad de decidir sobre el tratamiento. En este sentido, cobrará importancia el papel asesor de la AEPD cuando emite informe sobre las disposiciones generales que puedan considerarse que desarrollan la LOPD (art. 37.h LOPD).

Respecto al sector público nos hallamos con la tentación de atribuir la responsabilidad automáticamente al sujeto que detente la competencia. Sin embargo, como ya se indicó, el elemento subjetivo no debe corresponder necesariamente con la persona jurídica que detenta la competencia, ya que la administración pública se configura de una forma integral. En consecuencia, habría que ir más allá de esa titularidad para ver quien ostenta realmente la capacidad de decisión sobre el tratamiento. La determinación del responsable debería estar de acuerdo con el elemento subjetivo del concepto que permite el fraccionamiento por órganos de la responsabilidad. Así, Antonio

[437] A eso hay que añadir lo referido respecto al Considerando 47 Directiva 95/46/CE que afirmaba que el operador de telecomunicaciones normalmente no debía ser considerado responsable respecto a los datos transmitidos sino que el responsable era el emisor. No obstante, el operador sí será responsable de los datos de tráfico y otros datos relativos a la comunicación y al abonado. Además hay que tener en cuenta que en la legislación de telecomunicaciones se incluye las medidas establecida por la Directiva 2002/58/CE relativa a la privacidad de los servicios de comunicaciones electrónicas que complementa a la Directiva 95/46/CE.

[438] En el Informe de la AEPD 636/2009 se planteaba si un administrador de fincas podía proporcionar la lista de propietarios al presidente de una comunidad de propietarios. La clave para resolver la consulta es determinar cual es el papel del administrador de fincas y para ello la AEPD acude a la ley de propiedad horizontal. La finalidad del tratamiento de los datos de los propietarios debía enmarcarse en esta ley que establecía unas obligaciones para las comunidades. Por tanto, el responsable debe ser la comunidad de propietarios que es el sujeto obligado por la ley y el que debe decidir sobre el tratamiento. El administrador de fincas es un encargado del tratamiento porque lo que hace es prestar el servicio de administración a las comunidades de propietarios.

TRONCOSO REIGADA, sin perder de vista que lo esencial para determinar al responsable es la capacidad de decidir sobre el tratamiento, estima que esta capacidad corresponde al órgano titular de la función específica en que se concrete esa competencia material a cuyo ejercicio sirve instrumentalmente el fichero[439].

La determinación del responsable no es una cuestión fácil ni tampoco cuenta con una única solución. Sin embargo, como nos recuerda este mismo autor, hay que tener en cuenta que la LOPD no impone un modelo concreto de gestión, sino que es flexible en este sentido[440]. En consecuencia, lo importante es que, en caso de duda, se opte por el enfoque más garantista para la protección del derecho, especialmente en este ámbito del sector público, donde debe primar la protección del ciudadano. También debe acudirse a las características del elemento objetivo que pueden ayudar a determinar a quién corresponde esa capacidad de decisión. No será lo mismo si el fichero es manual o automatizado o si la forma de almacenamiento es centralizada o descentralizada.

[439] Así este autor aplica el criterio que ofrecía la derogada Ley 8/2001, de 13 de julio, de protección de datos de carácter personal en la Comunidad de Madrid que, además de incluir el concepto de responsable idéntico al de la LOPD, establecía, en su artículo 7, dedicado al responsable del fichero, los siguientes criterios de determinación del mismo: "1. Responsable del fichero es el órgano administrativo designado en la disposición de creación del fichero al que corresponde decidir sobre la finalidad, contenido y uso del tratamiento. 2. Cuando no sea posible la determinación del responsable del fichero, por estar atribuidas a diferentes órganos administrativos la competencia para decidir sobre la finalidad, contenido y uso del tratamiento, se entenderá por responsable del fichero al órgano titular de la función específica en que se concrete la competencia material a cuyo ejercicio sirva instrumentalmente el fichero. 3. En el caso de los Organismos Autónomos, Entidades de Derecho público y demás Entes públicos, y salvo que las normas fundacionales de los mismos dispongan otra cosa, el responsable del fichero será el Gerente o Director de aquellos." A. TRONCOSO REIGADA, *La protección de datos personales. En busca del equilibrio*, *op. cit.*, pág. 305.

[440] Se ilustra esta cuestión con las diferentes aproximaciones del autor y de la AEPD entorno al modelo de declaración de ficheros de los centros docentes públicos de enseñanza secundaria. La AEPD acude al criterio de la titularidad de la competencia y de la personalidad jurídica para entender que los centros docentes no tienen esta personalidad propia y que son órganos dependientes de la Consejería autonómica. En consecuencia le atribuye la capacidad de notificar y la responsabilidad a la Consejería y considera a los centros meros usuarios del fichero de datos. Informe 143/2004 de la AEPD. TRONCOSO REIGADA matiza esta atribución de responsabilidad, de forma que entiende que debe tenerse en cuenta que, en el caso del fichero de alumnos, la legislación establece una autonomía pedagógica, organizativa y de gestión económica, a la Dirección del centro docente, lo que le permite una cierta capacidad de decisión sobre finalidad, contenido y uso de los tratamientos. Esto será más claro si la información se encuentra en soporte papel o en una aplicación informática descentralizada que permitirá correspondencia entre fichero jurídico y fichero físico. Sin embargo, también puede ser lógico atribuir la responsabilidad a una Dirección General de la que dependan todos los centros educativos si existe un modelo informático centralizado. También puede ser la Consejería quien se atribuya la responsabilidad por entender que tiene atribuidas las competencias. Sin embargo, el autor indica que la competencia no es de esta Consejería sino de la propia Administración Autonómica. A. TRONCOSO REIGADA, *La protección de datos personales. En busca del equilibrio*, *op. cit.*, págs. 313, 1.288 a 1.293.

Con el fin de asegurar la máxima coherencia en la determinación del responsable y seguridad jurídica, es imprescindible que se incentiven los procesos reflexivos entorno a esta cuestión. Asimismo, este proceso debe materializarse en evidencias escritas, con el fin de facilitar el control del mismo. A ello ayuda el trámite de notificación de ficheros y la actitud asesora de las autoridades de control en esta fase previa[441]. De esta forma, es importante establecer estos mecanismos de prevención para evitar una atribución incorrecta de la responsabilidad.

ii. El poder de decidir emana de de una capacidad de influencia de hecho

Asimismo, como se indicó cuando se abordó el análisis del elemento funcional en la Directiva 95/46/CE, deberemos acudir, también, a la realidad para analizar si lo establecido en la normativa se traduce en la práctica en esa capacidad de decidir por parte del responsable. Y es que debe primarse lo que sucede realmente, antes que lo que en un plano teórico debería suceder. Así, si una norma establece que un sujeto tiene una función que implica que decida sobre unos datos personales pero, en la realidad, no es así, lo que debería tenerse en cuenta, a la hora de valorar si ese sujeto es responsable o no, es esta realidad.

Las autoridades de control tendrán que realizar este examen si les toca actuar. De esta forma, incluso en un tratamiento que se lleve a cabo en contra de las previsiones normativas, debe identificarse al responsable. Es más, en estos casos lo que debe prevalecer es precisamente quien actúa, sin perjuicio de que cumpla o incumpla la ley.

Pese al entorno fuertemente regulado en el que se mueven las organizaciones públicas y privadas, quedan espacios libres no sujetos a regulación, especialmente en el sector privado. Así, en este sector la creación de ficheros se permite cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona o empresa (art. 25 LOPD). En virtud de esta limitación queda claro que los tratamientos de datos que lleven a cabo los sujetos del sector privado se enmarcarán en su actividad negocial, por lo que, para determinar al responsable, podremos acudir a la documentación donde se describa

[441] Así, la ACPD, además de emitir informe preceptivo sobre los proyectos de disposiciones de carácter general de la *Generalitat* de creación, modificacón o supresión de ficheros, también lo hace de forma potestativa respecto a los proyectos de los entes locales (art. 5.m) y n) Ley catalana).

esta actividad, como es por ejemplo la escritura de constitución de la sociedad, donde obran los estatutos de la misma y debe constar la definición del objeto social.

Para determinar al responsable, podrán tomarse como indicios la documentación elaborada por el sujeto para adaptarse a la normativa, políticas y protocolos que definan procesos de trabajo, los contratos que puedan ser pertinentes, así como la documentación mercantil que defina la actividad de la persona jurídica. De nuevo, hay que subrayar la importancia que tendrá la creación de evidencias que reflejen esta responsabilidad, como pueden ser las instrucciones que establezca la organización respecto a los tratamientos de datos que se lleven a cabo[442].

b. Aspectos concretos sobre los que recae la capacidad de decisión del responsable: la finalidad, contenido y uso del tratamiento

Los aspectos concretos sobre los que decidirá el responsable son "la finalidad, contenido y uso del tratamiento". Por lo tanto, no coinciden exactamente con los señalados en el Convenio 108 y la Directiva 95/46/CE[443]. Respecto a esta última, el GA29 entendía que los fines y los medios sobre los que decidía el responsable debían responder a las preguntas "por qué" y "cómo"[444]. En el caso de "la finalidad, contenido y uso", en la LOPD, se equipararía la palabra "finalidad" a la de fines, respondiendo, por lo tanto a la pregunta "por qué" se lleva a cabo el tratamiento. En este supuesto queda claro que quién responda a esta pregunta es quién decide que se va a llevar a cabo el tratamiento y, por lo tanto, será el responsable.

No es tan coincidente el aspecto relativo a "medios" establecido por el legislador comunitario y las menciones a "contenido y uso" que realiza el legislador español. Si rescatamos los aspectos sobre los que decidía el responsable, según el texto de la Propuesta de Directiva de 1990 - la que existía cuando se elaboraba la LORTAD - eran: la finalidad del fichero, las categorías de datos personales que deben registrarse, las

[442] A. TRONCOSO REIGADA, *La protección de datos personales. En busca del equilibrio*, *op. cit.*, págs. 311 a 312.
[443] Hay que recordar que en el Convenio 108, la autoridad controladora del fichero decidía sobre la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán. La Directiva 95/46/CE establece que el responsable determina los fines y los medios del tratamiento de datos personales.
[444] Ver CAP II.

operaciones que deben aplicárseles a estos datos y a qué terceros está permitido el acceso a los mismos. Tampoco parece responder a esta enumeración la referencia a "contenido" y "uso". El término "uso" respondería también a la pregunta del por qué o el para qué se utilizan los datos exactamente[445]. El "contenido" correspondería a las categorías de datos que deben registrarse, de la Propuesta de Directiva de 1990.

Si se atiende a la interpretación literal del artículo 3.d) LOPD sería responsable el que decidiera sobre el "por qué" se realiza el tratamiento y sobre el contenido del fichero. No sería responsable el que decide sobre los medios utilizados en el tratamiento, es decir, sobre los demás aspectos del "cómo". Sin embargo, esta interpretación no seguiría la realizada por el GA29 que, además, entendió que la referencia a "fines y medios" era un resumen de la lista anterior. Por lo que la palabra medios incluiría la decisión sobre los datos personales a tratar, las operaciones a aplicar y los terceros a los que se dará acceso. Para ser coherente con la interpretación que el GA29 realiza del concepto de la Directiva 95/46/CE debería entenderse lo mismo respecto a la ley española.

No obstante, sin perjuicio de que estamos ante un concepto jurídico autónomo de derecho comunitario y como lo indicado por el GA29 no es vinculante, también cabe la opción de interpretar que la LOPD establece esos tres aspectos -la finalidad, el contenido y usos del tratamiento- como los esenciales sobre los que debe decidir el responsable. Así, por ejemplo, debería entenderse que los medios técnicos o los terceros que acceden a los datos no son esenciales.

Sin embargo, la normativa española ha regulado las medidas de seguridad que deben aplicarse a los datos, por lo que parece que su definición debe considerarse esencial. Por otro lado, no cabe duda que la transmisión a terceros de los datos debe considerarse también un elemento esencial, ya que este extremo exigirá el cumplimiento de una serie de requisitos estipulados en la legislación que debe cumplir el responsable.

[445] En el manual de ayuda para la notificación de ficheros de la AEPD, se incluye en el mismo apartado la descripción de las finalidades y usos del fichero. Manual del formulario electrónico de notificación de ficheros de titularidad privada, AEPD, 20.2.2013, pág. 11. En el Diccionario de la lengua española, de la RAE, 22ª ed., se define contenido como "cosa que se contiene dentro de otra" y uso, en su primera acepción, como "acción y efecto de usar" y usar es "hacer servir una cosa para algo".

Respecto a los criterios que se pueden utilizar para determinar si nos hallamos ante un responsable, se podrá acudir a los sugeridos por el GA29 que se examinaron anteriormente. No obstante, resulta interesante revisar los criterios que se han seguido en el marco de la legislación española, especialmente en la diferenciación entre responsable y encargado. De esta forma, donde se encuentran los aspectos que pueden tenerse en cuenta para calificar al responsable es sobre todo cuando se aborda un supuesto en el que debe optarse por calificar a un determinado sujeto como responsable o como encargado. Por ello, posteriormente se hará mención a esta delimitación.

c. Corresponsabilidad. Responsable del fichero vs. Responsable del tratamiento

El artículo 5.1.q) RLOPD vino a confirmar la posibilidad de que se dieran supuestos de corresponsabilidad, al añadir a la definición de responsable "que sólo o conjuntamente con otros decida". Por otro lado, también se especificó, en este artículo, que "aunque no lo realizase materialmente" (el tratamiento), también podría considerarse responsable del fichero o del tratamiento.

Con estas modificaciones, se alineaba el concepto con el de la Directiva 95/46/CE, al introducir la pluralidad de responsables. Sin perjuicio de la aplicación de los criterios esgrimidos sobre la corresponsabilidad, en el marco de la Directiva 95/46/CE[446], quiero hacer referencia a un caso específico de corresponsabilidad al que también responden estos cambios introducidos en el concepto. Y es que la normativa española ha originado entorno al responsable una doble figura: la del responsable del fichero y la del responsable del tratamiento[447]. La diferencia evidente es el objeto sobre el que recaerá la capacidad de decisión del responsable: el fichero o el tratamiento.

[446] Ver Capítulo II.

[447] Si bien DEL PESO NAVARRO entiende que esta doble figura responde a los postulados de una doctrina minoritaria y manifiesta su oposición a la existencia de esta singularidad, ya que no existen argumentos para defender la distinción. Asimismo, afirma que iría en contra de lo previsto por la Directiva 95/46/CE que sólo establece una figura. Este autor, sin embargo, considera que sería positivo que existieran dos figuras, el responsable o titular del fichero, que decidiría sobre éste y el responsable del tratamiento que realizaría el tratamiento. E. DEL PESO NAVARRO, M.A. RAMOS GONZÁLEZ, M. DEL PESO RUÍZ, M. DEL PESO RUÍZ, *Nuevo reglamento de protección de datos de carácter personal. Medidas de seguridad*, Díaz de Santos, Madrid, 2008, págs. 41 a 42.

i. La gestación parlamentaria

Esta especial regulación ha sido consecuencia de una serie de avatares producidos durante la elaboración de las leyes. En la LORTAD, la primera ley española de protección de datos, porque, al elaborarla, se partió del texto inicial del proceso de elaboración de la Directiva 95/46/CE, es decir, la Propuesta de Directiva de 1990. En este primer texto de 1990, al responsable se le calificaba como "del fichero", ya que en ese momento se vertebró la norma alrededor del concepto de fichero. Por eso, se eligió para nombrar al responsable en la LORTAD "del fichero" y así quedó fijado en el texto final. Sin embargo, el procedimiento de elaboración de la Directiva 95/46/CE fue largo y con un prolífico debate que dio lugar al cambio en este concepto vertebrador de la norma, que pasó de ser el fichero a ser el tratamiento, noción que se consideró más dinámica. La Directiva 95/46/CE acabó por nombrar al responsable "responsable del tratamiento".

Llegados a este punto, se inició en España el proceso de adaptación de la LORTAD a la Directiva 95/46/CE y, por lo tanto, había que abordar la cuestión relativa a la denominación del responsable, que ya no encajaba, en absoluto, con la que indicaba la Directiva 95/46/CE. Pero, en vez de sustituir la denominación "responsable del fichero" por la de "responsable del tratamiento", lo que además fue sugerido por el Grupo Parlamentario Vasco, se adoptó la denominación "responsable del fichero o del tratamiento", propuesta por el Grupo Socialista[448]. Este cambio no suscitó ningún inconveniente por parte de los diputados durante todo el trámite parlamentario, por lo que finalmente se aprobó en el texto definitivo de la LOPD[449].

[448] El Grupo Parlamentario Vasco (EAJ-PNV), mediante enmienda nº 18, sugirió, al inicio del debate parlamentario sobre la, en aquel momento, modificación de la LORTAD, que se cambiara el artículo 3.d) de esa ley (que contenía la definición de responsable) incluyendo "Responsable del tratamiento" en vez de "Responsable del fichero". De esta forma, señaló el grupo parlamentario, se adecuaría mejor la disposición al contenido de la Directiva 95/46/CE. Sin embargo, el Grupo Parlamentario Socialista presentó enmienda nº 47 en la que propuso que se indicara "Responsable del fichero o tratamiento". Enmiendas al Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (núm. 121/000135), BOCG, Congreso de los Diputados, VI Legislatura, Serie A: Proyectos de Ley, núm. 135-7, presentación de enmiendas, 4 de noviembre de 1998, págs. 21 a 22 y 30.

[449] Parece ser que es este término "Responsable del fichero o tratamiento" el que convence más a los diputados, que formaban parte de la Ponencia, encargada de redactar el Informe sobre el Proyecto de Ley por el que se modificaba la LORTAD, porque es la que escogen para el Proyecto. En ese momento la Ponencia había decidido cambiar el procedimiento y, en vez, de modificar la LORTAD se adoptó un nuevo texto que sería el de la LOPD. Por tanto, aún quedaba otra oportunidad para que el Grupo Parlamentario Vasco insistiera en incluir su enmienda nº 18. Sin embargo, la sra. Uría Echevarría, de este grupo, manifestó que esta enmienda había formado parte de un grupo de enmiendas de carácter técnico, cuyo objetivo había sido la mejor adecuación al lenguaje empleado por la Directiva 95/46/CE y para conformar

Esta dualidad en la denominación del responsable, junto a la eliminación, ya señalada, del término "tratamiento" de la definición de fichero, dio como resultado que la jurisprudencia entendiera que se trataba de dos sujetos diferenciados: el responsable del fichero que decidía sobre el fichero y el responsable del tratamiento que decidía sobre el tratamiento.

Ni el hecho de que en el marco sancionador no se especificara más que al responsable del fichero ni tampoco el hecho de que del análisis de la ley no se obtuviera un régimen diferenciado para ambas figuras, fueron un freno para esta doctrina jurisprudencial. De hecho, la primera sentencia, se puede decir, que se encontró de frente con un supuesto que encajaba perfectamente en esta hipótesis.

ii. La interpretación jurisprudencial y la regulación en el ámbito del sector publicitario

La primera sentencia que aplica la dualidad es la del Tribunal Supremo de 5 de junio de 2004, que deniega un recurso de casación para unificación de doctrina[450]. La sentencia recurrida había resuelto confirmar la sanción impuesta por la AEPD a una empresa que había encargado a otra el envío publicitario a 1.400 mujeres de una población de Valladolid[451]. La empresa contratada alquiló los datos a otra empresa. Una de las destinatarias del envío denunció este tratamiento de datos para el que no había otorgado su consentimiento a ninguna de las empresas implicadas.

La AEPD había considerado en su resolución que, pese a que la empresa que encargó el envío no era la que había creado el fichero, sí era la beneficiaria de la publicidad realizada y la que había encargado la campaña publicitaria. Por tanto, de

dentro del texto la figura del encargado del tratamiento. Pues bien, la parlamentaria afirmó que prácticamente todas estas enmiendas habían sido asumidas o íntegramente aceptadas, por lo que optó por no considerarlas objeto de defensa ni de sometimiento a votación. Informe de la ponencia sobre el Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (núm. 121/000135), BOCG, Congreso de los Diputados, VI Legislatura, Serie A: Proyectos de Ley, núm. 135-9, presentación de enmiendas, 14 de septiembre de 1999, pág. 60 y Dictamen de la Comisión Constitucional a la vista del informe elaborado por la Ponencia, sobre el Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (núm. 121/000135), Diario de Sesiones del Congreso de los Diputados, VI Legislatura, Comisión Constitucional, Sesión núm. 24 de 15 de septiembre de 1999, núm. 744, pág. 21875.

[450] STS de 5 de junio de 2004 (Sala 3ª) (ROJ: STS 3896/2004).

[451] SAN de 16 de octubre de 2003 (Sala de lo contencioso-administrativo) (ROJ: SAN 1936/2003).

acuerdo con la definición de responsable, tenía que considerarse responsable del tratamiento de los datos utilizados en la campaña y había cometido una infracción por tratarlos sin el consentimiento de la persona afectada[452].

La Audiencia Nacional confirmó esta interpretación de la AEPD, entendiendo que así lo permitía la LOPD. Si bien recordaba que la LORTAD ceñía su ámbito de aplicación al fichero automatizado y, por tanto, se limitaba a definir al responsable del fichero, indicaba que, en la LOPD, esto cambió. Así la Audiencia argumentó que se había modificado la definición de fichero, de la que se excluyó toda referencia al tratamiento[453] y se diferenció entre las figuras de responsable del fichero y responsable del tratamiento[454]. Según la Audiencia Nacional:

> "el responsable del fichero es quien decide la creación del fichero y su aplicación, y también su finalidad, contenido y uso, es decir quien tiene capacidad de decisión sobre la totalidad de datos registrados en dicho fichero. El responsable del tratamiento, sin embargo, es el sujeto al que cabe imputar las decisiones sobre las concretas actividades de un determinado tratamiento de datos, esto es, sobre una aplicación específica. Se trataría de todos aquellos supuestos en los que el poder de decisión debe diferenciarse de la realización material de la actividad que integra el tratamiento."[455]

Este razonamiento, seguido por la Audiencia Nacional, diferenció el poder de decisión de la realización material. Por lo tanto, se distinguió al responsable que realmente decidía en este supuesto concreto, del tratador efectivo, que lo que hacía era llevar a cabo materialmente el tratamiento. Este tratador efectivo que podría haber sido calificado como encargado del tratamiento se estimó, sin embargo, que era otro responsable: el responsable del fichero.

---

[452] Resolución de la AEPD de 27 de julio de 2001 que desestimó el recurso de resposición interpuesto contra la resolución de la AEPD de 23 de mayo de 2001 y que impuso a Club Internacional del Libro, División de Crédito SA una multa de diez millones de pesetas, de acuerdo con el artículo 45.2 LOPD, por infracción del artículo 6.1 LOPD relacionado con el artículo 3.d) LOPD, tipificada como grave en el artículo 44.3.d) LOPD. SAN de 16 de octubre de 2003 (Sala 1ª) (ROJ: SAN 1936/2003), FJ 1.

[453] La Audiencia Nacional al esgrimir la modificación de la definición del fichero cita el artículo 2 LOPD, en vez del artículo 3.b) donde se encuentra este concepto. *Ibídem*, FJ 3.

[454] También añade que se delimitaba con precisión la figura del encargado del tratamiento. No obstante, al manifestar la diferencia entre los dos responsables, la Audiencia cita los apartados b y d del artículo 3. En el apartado d) se encuentra la definición de "responsable del fichero o del tratamiento", por lo que sería adecuada su cita pero en el apartado b) lo que se encuentra es la definición de "fichero", por lo que no sería pertinente su cita. *Ibídem.*

[455] *Ibídem.*

La Audiencia Nacional también se remitió, en su sentencia, al concepto que establece la Directiva 95/46/CE de "responsable del tratamiento" para enfatizar la diferenciación entre éste y el responsable del fichero, diferenciación que había surgido con el artículo 3 LOPD, en función de si el poder de decisión se dirigía al fichero o al tratamiento. En consecuencia, la interpretación del concepto de la Directiva 95/46/CE, en vez de servir para alinear la LOPD con la norma europea y realizar un enfoque integrador del responsable, lleva a la Audiencia a verificar la distinción entre ambas figuras.

El Tribunal Supremo acogió esta tesis y denegó la identidad de las sentencias de contraste aportadas porque, entre otras cosas, se referían a la regulación establecida en la LORTAD en la que no se preveía, según el Alto tribunal, la diferenciación entre estas dos figuras[456]. Pero, además, especificó que el título VII de la LOPD dedicado a regular las infracciones y sanciones, establecía claramente que "los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente ley" (art. 43 LOPD), lo que entendió que confirmaba lo argumentado por la Audiencia Nacional[457].

[456] STS de 5 de junio de 2004 (Sala 3ª) (ROJ: STS 3896/2004), FJ 4.

[457] Esta doctrina se recoge también, de forma aún más tajante, en STS de 28 de febrero de 2005 (Sala 3ª) (ROJ: STS 1234/2005) y en la STS de 26 de abril de 2005 (Sala 3ª) (ROJ: STS 2570/2005), que retoman lo allí indicado. De esta forma, el Tribunal Supremo afirma que "El problema de la carencia de identidad sustancial aparece extensamente tratado por el Abogado del Estado en sus alegaciones de oposición, donde expone con claridad la radical innovación que supuso –respecto de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento de datos de carácter personal, por infracción del artículo 43.3.d) mientras que la sentencia impugnada versa sobre la adecuación a derecho de la sanción impuesta en aplicación de la Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal, por infracción del artículo 44.3.d). Pero es el caso que junto al responsable del fichero –que era en la Ley 5/1992- quien estaba sujeto al régimen sancionador establecido en dicha ley (art. 42) en la nueva Ley 15/1999 aparece un nuevo personaje, el responsable del tratamiento, como posible sujeto pasivo de la potestad sancionadora de la que hoy se llama –a partir de la Ley 62/2003, de 30 de diciembre –Agencia Española de Protección de Datos (artículo 43). Véase lo que dice uno y otro precepto: Ley 5/1992 "Art. 42. Responsables: 1. Los responsables de los ficheros estarán sujetos al régimen sancionador establecido en la presente ley". Ley 15/1999"Art. 43. Responsables: 1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente ley". Y esto es así porque la nueva Ley Orgánica –a diferencia de la vieja Ley Orgánica, que atribuía la potestad de decidir sobre la finalidad, contenido y uso del tratamiento únicamente al responsable del fichero- reconoce que esa decisión pueda tomarla –y así ocurre muchas veces- el responsable del tratamiento. He aquí el nuevo texto: Ley 15/1999. "Artículo 3. A los efectos de la presente Ley se entenderá por: […] d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento". No se trata como se ve de un mero cambio de redacción, de un simple giro gramatical, o una innovación puramente estilística. Es algo más profundo: estamos ante un cambio esencial en el modo de afrontar la regulación de las relaciones que se entablan entre quienes manejan los datos y el titular de los mismos." STS de 28 de febrero de 2005 (Sala 3ª) (ROJ: STS 1234/2005), FJ 4.

Resulta sorprendente que el Alto Tribunal entendiera, en virtud de lo indicado en el artículo 43 LOPD, que los responsables del tratamiento estaban sujetos al marco sancionador de la ley, cuando no aparecen nombrados de ninguna forma. A eso hay que añadir que esa afirmación no se acompañó de ninguna motivación que permitiera comprender el razonamiento del tribunal[458].

Independientemente de la motivación que esté detrás de esta doctrina, la cuestión es que el Tribunal Supremo constató la creación de una nueva figura: el responsable del tratamiento.

Esta dualidad en la figura del responsable se enfrenta con el hecho de que, en su definición, como ya se ha apuntado anteriormente, la determinación del mismo radica en la capacidad de este sujeto de decidir respecto al tratamiento, no respecto al fichero. En consecuencia, tanto si estamos ante el responsable del fichero, como si estamos ante el responsable del tratamiento, ambos deberían decidir sobre el tratamiento. Un sujeto que no decide sobre el tratamiento, no entraría en la definición y no debería ser considerado responsable, de acuerdo con la LOPD.

En el caso planteado, se tendría que haber calificado tanto al que encarga la campaña publicitaria, como a quien la lleva a cabo, corresponsables porque ambos deciden sobre el tratamiento. El beneficiario de la campaña decide sobre la finalidad y también sobre el contenido del tratamiento, al determinar los criterios para elegir a los destinatarios de la campaña. El que la lleva a cabo mediante un fichero que ha creado él mismo, también ha decidido previamente sobre qué datos incluir en el mismo y para qué se van a destinar. Si este prestador realiza el servicio mediante la subcontratación de otro a quien alquila la base de datos para realizar la campaña también decide sobre los usos de los datos.

[458] Y es que podría optarse por diversas posturas que podrían explicar esta conclusión del Tribunal Supremo. Así, podría haber sido fruto de una confusión entre las figuras del encargado del tratamiento y del responsable del tratamiento. También podría deberse a que el Tribunal Supremo entendiera que, al existir encargado del tratamiento, debería existir un responsable de ese tratamiento que debe incluirse como sujeto merecedor de sanción en caso de vulneración. Por último, el Alto Tribunal podría haber considerado que el hecho de no repetir la alusión a "responsable del fichero o del tratamiento" que se encontraba en la definición del mismo en el artículo 3.d) LOPD debía ser consecuencia de un olvido del legislador que debía repararse y considerar que estas dos figuras que había diferenciado la Audiencia Nacional debían considerarse incluidas en el artículo 43 LOPD (hipótesis que es la que parece más probable).

Esta doctrina se trasladó al RLOPD, de forma que se incluyó la figura del responsable del tratamiento claramente en la regulación dedicada a los tratamientos de datos para actividades de publicidad y prospección comercial (art. 45 ss. RLOPD). Esta regulación desarrollaba el artículo 30 LOPD, que se enmarca en las disposiciones específicas de los ficheros de titularidad privada. Así, se dirige la regulación a aquellas empresas que quieran realizar una de estas campañas respecto a sus productos y servicios. Es el supuesto en el que estas empresas opten por contratar a un tercero donde, como ya se ha visto en la jurisprudencia analizada, entrará en juego el responsable del tratamiento. Las normas a aplicar serán:

> "a) Cuando los parámetros identificativos de los destinatarios de la campaña sean fijados por la entidad que contrate la campaña, ésta será responsable del tratamiento de los datos.
> b) Cuando los parámetros fueran determinados únicamente por la entidad o entidades contratadas, dichas entidades serán las responsable del tratamiento.
> c) Cuando en la determinación de los parámetros intervengan ambas entidades, serán ambas responsables del tratamiento." (art. 46.2 RLOPD)

A estas normas se añade, lo que debe considerarse "parámetros identificativos de los destinatarios" que serán "las variables utilizadas para identificar el público objetivo o destinatario de una campaña o promoción comercial de productos o servicios que permitan acotar los destinatarios individuales de la misma." (art. 46 RLOPD).

Lo primero que hay que señalar es que no se sigue al pie de la letra la doctrina del Tribunal Supremo ya expuesta, ya que no se deja clara la dualidad responsable del fichero/responsable del tratamiento. Debido al giro en la regulación debería haberse clarificado más el juego de estas dos figuras.

Lo que se extrae de estas previsiones es que la asignación del papel de responsable del tratamiento depende de quién decide sobre un aspecto concreto que entiendo que afectaría al contenido del tratamiento: los parámetros identificativos de los destinatarios[459]. Sin embargo, la necesidad de crear la doble figura surgió porque el fichero había sido creado y estaba bajo el directo poder de la empresa contratada para

[459] Como indican PENDÓN MELÉNDEZ y GÁLLEGO HIGUERAS la determinación de los parámetros identificativos de los destinatarios de la campaña, supone una selección indirecta de las personas a quienes se dirigirá la publicidad, lo que puede hacerse sin tener acceso material a los datos, lo que es característico de la figura del responsable del tratamiento. M.A. PENDÓN MELÉNDEZ, G.F. GÁLLEGO HIGUERAS, "Tratamientos con fines de publicidad y de prospección comercial", A. TRONCOSO REIGADA (Dir.). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, pág. 1.671.

realizar la campaña publicitaria por el anunciante. Se trataba pues de un responsable del fichero que era contratado por una empresa anunciante, que no accedía a los datos en ningún momento.

El Tribunal Supremo lo que determinó es que el anunciante era responsable del tratamiento porque era, en virtud de su capacidad de decidir sobre esa concreta campaña, la razón por la que se realizaba el mismo. Sin embargo, el prestador de servicios publicitarios era responsable del fichero.

Pues bien, al centrarse esta regulación establecida en el artículo 46.2 RLOPD únicamente en la figura del responsable del tratamiento, no queda claro si se parte de que el fichero está en manos del prestador del servicio o si es que esta cuestión no se considera controvertida y, por ese motivo, se ha dejado fuera de la regulación.

La pregunta que cabría hacerse es ¿si el fichero está en manos del anunciante se aplicará en todo caso este precepto? Si el anunciante contratara a una entidad para que lleve a cabo una campaña y determine los parámetros identificativos de los destinatarios, si aplicamos lo establecido en esta disposición, tendrá que considerarse responsable del tratamiento a esta empresa contratada, independientemente de que la responsable del fichero sea la anunciante. En caso contrario, sería admitir que lo importante para atribuir la responsabilidad sería quién detenta el fichero y no tendría sentido establecer un criterio que debe estar conectado con el concepto de responsable. De esta forma, si una empresa decide sobre un elemento esencial, como es el contenido del tratamiento, deberá ser considerado responsable.

Sin embargo, un argumento que parece estar en contra de esta interpretación es la imposición al anunciante de la obligación de adoptar las medidas necesarias para asegurarse de que la empresa contratada haya recabado los datos, de acuerdo con la LOPD y el RLOPD (art. 46.3 RLOPD). Esta disposición parte de que la empresa contratada ha recabado los datos, por lo que podría asumirse que si los recaba es que debe ser la responsable del fichero[460].

[460] La AEPD estima que si el anunciante es responsable del fichero y los datos de los destinatarios proceden únicamente de este fichero no debería aplicarse el artículo 46.2 RLOPD. Este precepto sólo se aplicará si se cumplen dos premisas: que se encomiende a un tercero la realización de una campaña y que la

iii. La interpretación jurisprudencial y la regulación en el sector de la solvencia patrimonial y el crédito

Los servicios sobre información relativa a la solvencia de las personas pueden implicar graves perjuicios a los afectados, si no gestionan correctamente los datos, al limitar la capacidad de éstos para poder contratar o solicitar créditos. Muestra de ello es que cuando se puso en marcha la AEPD, en 1994, enseguida destacó este sector como el que fue objeto de más denuncias por parte de los ciudadanos[461]. Como consecuencia de la especial problemática suscitada la AEPD adoptó su primera Instrucción en 1995 que establecía una regulación específica sobre este tipo de tratamientos[462]. Esta materia, como veremos ha sido también la que ha ocasionado más demandas de indemnización originadas por el incumplimiento de la normativa de protección de datos[463].

No es de extrañar que se incluyera, ya en la LORTAD, un precepto dedicado a este tipo de servicios (art. 28 LORTAD), que se mantuvo en la LOPD (art. 29 LOPD), pese a que no se incluía en la Directiva 95/46/CE. Esta regulación se incluye en la parte especial dedicada a los ficheros de titularidad privada y se ha desarrollado en el RLOPD

---

determinación de los destinatarios no proceda, o proceda solamente en parte, de ficheros de los que es responsable el propio beneficiario de la publicidad. Informe 295/2009 AEPD. Tampoco estiman aplicable este precepto a casos en los que el responsable del fichero sea el anunciante PÉNDON MELÉNDEZ y GÁLLEGO HIGUERAS. Estos autores consideran que la empresa contratada, en realidad no tendrá capacidad de decisión, si es el cliente quien tiene el fichero, ya que en último término el cliente puede aceptar o rechazar la propuesta de criterios que le haga la empresa contratada. Sin embargo, entiendo que, en el caso en el que el cliente no siga los criterios establecidos por la empresa contratada, el cliente decidirá y deberá ser calificado como responsable del tratamiento. En consecuencia, si la empresa cliente atiende a los criterios que establece la empresa contratada, debería considerarse a ésta responsable del tratamiento y aplicarse el precepto. M.A. PENDÓN MELÉNDEZ, G.F. GÁLLEGO HIGUERAS, "Tratamientos con fines de publicidad y de prospección comercial", A. TRONCOSO REIGADA (Dir.). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, págs. 1.682 a 1.684.

[461] En sus memorias de 1994 y 1995, la AEPD informaba que alrededor de la mitad de las denuncias recibidas eran sobre este sector (si bien es cierto que en aquel momento sólo hubieron un total de 81 denuncias). Memoria 1994 y Memoria 1995 AEPD. Cabe recordar que en el origen de la regulación sobre tratamiento de datos se encontraba una norma estadounidense de los años setenta dirigida, precisamente, a establecer las pautas del manejo de los datos sobre solvencia de los ciudadanos de EEUU, la *Fair Credit Reporting Act*. Ver capítulo I. También hay que mencionar que la LORTAD, en su exposición de motivos también hacía referencia a que: "El conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expresión del honor; y el perfil, sin duda, puede resultar luego valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión en ciertos colectivos".

[462] Instrucción 1/1995, de 1 de marzo, de la Agencia de Protección de Datos, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito, que se entiende derogada al aprobarse la LOPD.

[463] Ver Capítulo VII.

(arts. 37 ss.). Principalmente se limitan las fuentes a las que los prestadores de este tipo de servicios pueden acudir para obtener la información sobre la solvencia, se establecen los requisitos para que estos prestadores puedan tratar los datos y la forma en la que los afectados podrán ejercer sus derechos respecto a estos ficheros.

Los prestadores de este tipo de servicio pueden obtener los datos sobre solvencia de registros y fuentes accesibles al público, del propio interesado o de acreedores. Respecto a esta tercera vía, uno de los supuestos de vulneración de la legislación de protección de datos más habituales lo ocasionaba el acreedor, que proporcionaba datos incorrectos al prestador. Así, por ejemplo, el acreedor atribuía una deuda al afectado y no era cierto porque ya se había cancelado o porque no existía. De esta forma, no se respetaba el principio de calidad de los datos, ya que estos no eran exactos.

Mientras estuvo vigente la LORTAD, los tribunales entendieron que no podían sancionar a este acreedor informante, ya que no se le consideraba responsable del fichero[464]. El fichero común o fichero de morosos, donde se incluían estos datos, lo creaban y mantenían los prestadores de estos servicios. En la LORTAD, como ya se ha visto, el responsable del fichero era la única persona a la que podía exigirse responsabilidades. Tras la aprobación de la LOPD, se aplicó la doctrina jurisprudencial referida anteriormente y se consideró que el acreedor, pese a que no tiene poder de decisión sobre el fichero en su totalidad, sí debe ser considerado responsable del tratamiento con relación a la información que proporciona[465].

Entonces ¿por qué el artículo 29.3 LOPD considera que quien puede comunicar los datos que obran en el fichero (que no puede ser otro que el responsable del fichero común) es el responsable del tratamiento? Para que fuera coherente esta disposición con la doctrina expuesta debería referirse al responsable del fichero[466]. Y es que del análisis

[464] Así lo indica también M. GEIJO CASTANYA, "Prestación de servicios de información sobre solvencia patrimonial y crédito", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, págs. 1.592 a 1.593.

[465] Citar como ejemplo la STS de 18 de julio de 2006 (Sala 3ª) (ROJ: STS 4510/2006), FJ 1, que se refiere a la sentencia de instancia en la que se recogía exactamente la doctrina ya comentada sobre la existencia en la LOPD de las dos figuras, el responsable del fichero y el responsable del tratamiento. Entendía esta sentencia que el responsable de proporcionar el dato al fichero común es responsable de que este dato sea correcto y cumpla con el principio de calidad, al considerar que es responsable del tratamiento.

[466] Así, el artículo 29.3 LOPD establece que "(…)cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan

del texto de la LOPD no se puede extraer la lógica seguida para que, en algunas ocasiones se aluda al responsable del fichero y, en otras, se aluda al responsable del tratamiento ni tampoco parece seguir la de la jurisprudencia[467].

Al desarrollar la LOPD, se incluyó una extensa regulación de este tipo de ficheros en el RLOPD. Era de esperar que en esta norma, que era posterior al establecimiento de la doctrina referenciada, las alusiones a las empresas acreedoras informantes dejaran claro que se consideraban responsables del tratamiento. Sin embargo, en toda esta regulación no se nombra esta figura y al acreedor informante se le identifica como "el acreedor o quien actúe por su cuenta o interés". En cambio, sí se califica a los prestadores de servicios como responsables del fichero común[468]. Entiendo que, el hecho de calificar a los acreedores, de forma expresa, como responsables del tratamiento, sería contradictorio con la alusión comentada del artículo 29.3 LOPD que califica como tal al responsable del fichero común[469].

De esta forma, si bien en el artículo 43 RLOPD se establece la responsabilidad de los acreedores respecto al cumplimiento de los requisitos previstos en el RLOPD para poder notificar los datos adversos al responsable del fichero común, se limita a indicar que será "responsable de la inexistencia o inexactitud de los datos que hubiera facilitado para su inclusión en el fichero, en los términos previstos en la Ley Orgánica 15/1999"[470]. No se establece, por tanto, que se les considere responsables del tratamiento de forma expresa.

---

sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos."

[467] PENDÓN MELÉNDEZ y GÁLLEGO HIGUERAS indican el "nulo rigor" con el que la LOPD y el RLOPD utilizan los términos responsable del fichero y responsable del tratamiento. M.A. PENDÓN MELÉNDEZ, G.F. GÁLLEGO HIGUERAS, "Tratamientos con fines de publicidad y de prospección comercial", A. TRONCOSO REIGADA (Dir.). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, pág. 1.672.

[468] Si bien, para completar la confusión terminológica, el artículo 44 RLOPD también lo denomina como "titular del fichero común".

[469] Esto tiene como consecuencia que PRATS ALBENTOSA se refiera indistintamente a este responsable, como responsable del tratamiento o responsable del fichero. L. PRATS ALBENTOSA, "Régimen jurídico de los ficheros de solvencia", L. PRATS ALBENTOSA, M. CUENA CASAS (Coord.), *Préstamo responsable y ficheros de solvencia*, Aranzadi, Cizur Menor (Navarra), 2014, pag. 366.

[470] El artículo 43 RLOPD que se titula "Responsabilidad" establece: "1. El acreedor o quien actúe por su cuenta o interés deberá asegurarse que concurren todos los requisitos exigidos en los artículos 38 y 39 en el momento de notificar los datos adversos al responsable del fichero común. 2. El acreedor o quien actúe por su cuenta o interés será responsable de la inexistencia o inexactitud de los datos que hubiera facilitado para su inclusión en el fichero, en los términos previstos en la Ley Orgánica 15/1999, de 13 de diciembre."

En la regulación de la corresponsabilidad entre acreedor y responsable del fichero común, el RLOPD modula la responsabilidad de éste último, ya que establece que si recibe una solicitud de ejercicio de derechos de acceso, rectificación, cancelación u oposición referente a datos que haya proporcionado un acreedor, será suficiente que traslade la solicitud a este acreedor para que la resuelva (art. 44.3.1 RLOPD). Se exime a este responsable de responder la solicitud, a no ser que el acreedor no contestara en siete días y entonces podrá rectificar o cancelar cautelarmente los datos.

El Tribunal Supremo, en sentencia de 21 de mayo de 2014, exige del titular del fichero común una responsabilidad acorde con lo que establece la LOPD, la Directiva 95/46/CE, el Convenio 108 y la Carta UE[471]. En definitiva, el Alto Tribunal establece que, en sede civil, se demande del titular del fichero común una responsabilidad plena, sin posibilidad de modulaciones en virtud de una norma reglamentaria. En este caso, el responsable del fichero común había cumplido con este precepto, trasladó la solicitud de cancelación de los datos al acreedor y éste confirmó la exactitud de los datos, lo que comunicó el responsable al supuesto deudor[472]. Si bien los datos habían resultado incorrectos, el juzgado de instancia había absuelto al responsable del fichero común, que había seguido lo establecido en la normativa.

El Tribunal Supremo no hace ninguna referencia a la dualidad responsable del fichero/responsable del tratamiento en la sentencia pero afirma rotundamente que:

> "Como responsable del tratamiento de los datos obrantes en el registro de morosos del que es titular (Equifax), le compete atender la solicitud de cancelación o rectificación del afectado cuando la misma sea suficientemente fundada porque los datos incluidos en el fichero no respetan las exigencias de calidad derivadas de las normas reguladoras del derecho. Y por las mismas razones ha de responder de los daños y perjuicios causados al afectado cuando se haya incumplido estas obligaciones."[473]

El Tribunal Supremo constata que Equifax no es un mero encargado del tratamiento sino que es responsable del fichero común y del tratamiento de los datos en él incluidos, en los términos previstos en el artículo 2.d Directiva 95/46/CE y 3.d LOPD. Finalmente condena a ambas entidades, acreedor y responsable del fichero común como corresponsables solidarios.

[471] STS de 21 de mayo de 2014 (Sala 1ª) (ROJ: STS 267/2014), FJ 8.
[472] *Ibídem*, FJ 1.
[473] *Ibídem*, FJ 8.

Aunque la constatación del Alto tribunal se constriña al orden civil, hay que considerar el riesgo que, en general, una modulación de las obligaciones y, en consecuencia, de la responsabilidad supone para la protección de los derechos de los interesados. En concreto esta modulación se ve favorecida por la creación de estas dos figuras de responsable ya que ello implica una diferenciación entre ambos sujetos y, específicamente, respecto a sus obligaciones. Por tanto, esta modulación puede derivar en una restricción injustificada del derecho a la protección de datos que estuviera en contra de su regulación constitucional, convencional, internacional, comunitaria y legal, como ha estimado el Tribunal Supremo, respecto a la que se establecía en el RLOPD, una norma reglamentaria[474].

iv. Una tendencia expansiva de la dualidad interrumpida

Esta dualidad en la figura del responsable español, sin duda, vino a aumentar la complejidad entorno a la cuestión de determinar quién puede ser el responsable. No obstante, parecía que la utilización de este nuevo concepto se iba a acotar a dos ámbitos muy concretos de la actividad empresarial: la publicidad y los servicios de información sobre solvencia patrimonial y crédito.

No obstante, se trata de una figura que se fundamenta en la definición del artículo 3.d) LOPD y, por tanto, en una disposición de ámbito general. No es extraño que los tribunales y las autoridades de protección de datos la hayan utilizado para asignar responsabilidades en otros ámbitos, especialmente en el contexto de Internet. Esto ha permitido aplicar la normativa española en supuestos en los que, de otra forma, no hubiera sido posible o hubiera planteado dificultades.

Así se ha considerado que una persona que colgó un vídeo en el portal *Youtube* era responsable del tratamiento respecto a los datos incluidos en el mismo,[475] o que una empresa que utiliza las redes sociales para su actividad comercial es responsable del tratamiento, a no ser que obtenga los datos de estas redes sociales y los incluya en sus

[474] *Ibídem*, FJ 8.
[475] SAN de 20 de octubre de 2011(Sala de lo contencioso-administrativo) (ROJ: SAN 5251/2011).

propios ficheros, momento en el que se consideraría responsable del fichero[476]. En ambos casos, se consigue atribuir responsabilidad a un sujeto que se ubica en territorio español, ya que quien sería considerado responsable del fichero (*Youtube* o la red social) en el contexto de Internet será habitualmente una empresa ubicada en el extranjero. De esta manera, se evitan los problemas de la aplicación territorial de la LOPD[477].

Asimismo, el concepto de responsable del tratamiento se puede considerar de aplicación en el ámbito de la videovigilancia respecto a los sistemas que no graban las imágenes sino que sólo emiten las mismas en tiempo real. En estos casos no existe fichero, sino que sólo habría tratamiento de los datos[478]. En las Instrucciones que las autoridades de control han emitido sobre esta materia, dejan claro que la única diferencia respecto a las obligaciones que hay que cumplir, es que no será necesario notificar el fichero inexistente. También hay que resaltar que en estas Instrucciones no se menciona que, cuando estemos en este caso, en el que no hay fichero, debamos entender que estamos ante un responsable del tratamiento, diferenciado del responsable del fichero[479].

Y es que, pese a los casos citados, esta tendencia expansiva en el uso de la doble figura parece haberse detenido. Esta paralización en su aplicación sería coherente con la inminente reforma de la Directiva 95/46/CE, que supondrá la aprobación de un reglamento europeo que no permitirá aplicar esta doble figura.

2.3.4. Delimitación del concepto de responsable en contraposición con el de encargado del tratamiento

Los mismos criterios y características mencionados cuando se abordó la figura del encargado del tratamiento, en el marco de la Directiva 95/46/CE, serían aplicables en el ámbito español. Sin embargo, como se verá, la legislación española ha elaborado una regulación específica que ha erigido al encargado del tratamiento en figura también muy

[476] Informe 241/2011 de la AEPD.
[477] Ver Capítulo IV.
[478] Arts. 1.1 y 7.2 Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras (BOE núm. 296, 12.12.2006, pág. 43458-43460) y arts. 2, 9.1, 11.2 Instrucción 1/2009, de 10 de febrero, de la *Autoritat Catalana de Protecció de Dades*, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia, (DOGC, núm. 5322, 19.2.2009, págs. 13258-13272).
[479] Así, la Instrucción 1/2006 se refiere al "responsable" en casi todo su articulado y la Instrucción 1/2009 menciona como sujeto obligado al "responsable del tratamiento" en todo caso.

relevante en esta normativa. A esta relevancia ha contribuido el uso generalizado de la subcontratación, tanto en el sector público, como en el privado. Es normal que adquiera un papel mayor en la legislación nacional que en la Directiva 95/46/CE, ya que su existencia se debe a una necesidad de la práctica.

De esta forma, si se retoman los aspectos que hacían del responsable una figura clave en la legislación de protección de datos, se puede hacer un paralelismo con la figura del encargado. Así, el encargado del tratamiento español dispone de un auténtico estatuto que recoge una serie de obligaciones más amplias que las establecidas en la Directiva 95/46/CE[480]. Además, se configura como un criterio de aplicación de la normativa española a un tratamiento en lo referente a las medidas de seguridad, como también se establecía en la Directiva 95/46/CE[481]. Por último, a diferencia de la Directiva 95/46/CE, en la LOPD se establece claramente que el encargado podrá ser sancionado e, incluso, deberá indemnizar al titular de los datos[482]. Indiscutiblemente, los aspectos señalados tienen menos alcance que los que se refieren al responsable, pero no dejan de subrayar su función en esta normativa.

También, hay que destacar la especial configuración del encargo del tratamiento en la legislación española como un régimen excepcional que evita la aplicación de la regulación de la cesión de datos[483]. Esto implica que deban cumplirse de forma estricta las garantías que establece la legislación ya que, en caso contrario, se aplicaría el régimen general de la cesión al supuesto de hecho.

a. El análisis del concepto de encargado del tratamiento

La legislación española incluyó expresamente el concepto de encargado del tratamiento en la LOPD (art. 3.g), definición que es idéntica a la de la Directiva

[480] Y es que resulta elocuente que en la Directiva 95/46/CE la regulación del encargado del tratamiento se recoge en el artículo 17 relativo a la "seguridad del tratamiento", mientras que en la LOPD tiene una regulación dedicada a esta figura que se encuentra en su artículo 12 y que se ha desarrollado en los artículos 20 a 22 RLOPD. Además, el encargado, como no podía ser de otra forma, también tiene un papel clave en la regulación de las medidas de seguridad que se contiene en el Título VIII RLOPD. Ver Capítulo VI.
[481] Ver Capítulo IV.
[482] Ver Capítulo VII.
[483] La Directiva 95/46/CE no contiene una regulación específica para la cesión de datos y además incluye al encargado del tratamiento en su regulación de la seguridad del tratamiento. Por tanto, ambas regulaciones, la española y la europea, difieren en la forma de utilizar la figura.

95/46/CE[484]. No obstante, esta definición se alteró cuando se incluyó en el RLOPD (art. 5.1.i). El elemento subjetivo se cambió y en vez del que figuraba en la LOPD: "persona física o jurídica, autoridad pública, servicio o cualquier otro organismo", se incluyó el siguiente redactado: "persona física o jurídica, pública o privada, u órgano administrativo". Además, se añadió la mención de que pueden ser encargados del tratamiento "los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados". Así, lo que se perseguía era equiparar los elementos subjetivos de las definiciones de encargado y de responsable.

En esta definición ampliada se concreta que el encargado tratará datos por cuenta del responsable "como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio"[485]. Por eso, queda claro en la regulación española que esta definición no será aplicable a los empleados. El añadido relativo a la delimitación de la actuación del encargado que debe ser la prestación del servicio que le vincula al responsable, enlaza con la importancia que se ha otorgado a la extensión de la legitimación del tratamiento. Así, se ha entendido que la legitimación que tiene el responsable, para realizar el tratamiento, se extiende al tratamiento que lleva a cabo el encargado, siempre que se cumplan las garantías establecidas en la LOPD y en el RLOPD[486].

---

[484] Si bien en la LORTAD, en su artículo 27 se regulaba la prestación de servicios de tratamiento automatizado de datos de carácter personal limitando a estos prestadores que no podían aplicar o utilizar los datos obtenidos con fin distinto al que figure en el contrato de servicios, ni cederlos, ni siquiera para su conservación, a otras personas. También se contemplaba la obligación por parte de estos proveedores de, una vez cumplida la prestación contractual, destruir los datos personales, salvo que mediara autorización expresa de aquél por cuenta de quien se prestan tales servicios, porque razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podían almacenar con las debidas condiciones de seguridad por un período de cinco años.

[485] También en el artículo 12 LOPD quedaba patente que la aplicación de esta figura era a la prestación de servicios.

[486] Así la Audiencia Nacional ha indicado que: "Tal diferencia entre encargo de tratamiento y cesión, sin embargo, y como reconoce la doctrina, en algunos casos es compleja, pero lo que es indudable es que no puede haber cesión cuando existe encargo de tratamiento y no resulte preciso el consentimiento del afectado. Lo típico del encargo de tratamiento es que un sujeto externo o ajeno al responsable del fichero va a tratar datos de carácter personal pertenecientes a los tratamientos efectuados por aquél con el objeto de prestarle un servicio en un ámbito concreto. Habría por tanto encargo de tratamiento en los supuestos de *outsourcing* o en los de prestación derivada de un contrato de obra o arrendamiento de servicios con un fin concreto. Siendo esencial, para no desnaturalizar la figura, que el encargado del tratamiento se limite a realizar el acto material de tratamiento encargado, y no siendo supuestos de encargo de tratamiento aquellos en los que el objeto del contrato fuese el ejercicio de una función o actividad independiente del encargado. En suma, existe encargo de tratamiento cuando la transmisión o cesión de los datos está amparada en la prestación de un servicio que el responsable del tratamiento recibe de una empresa externa o ajena a su propia organización, y que le ayuda en el cumplimiento de la finalidad del tratamiento de datos consentida por el afectado." SAN de 13 de abril de 2005 (Sala de lo contencioso-administrativo) (ROJ: SAN 6766/2005), FJ 4. También cabe citar SAN de 20 de septiembre de 2002 (Sala de lo contencioso-

Por último, ya se ha comentado la creación en la normativa española de la doble figura del responsable (responsable del fichero y responsable del tratamiento). Esta doble figura supuso que el RLOPD especificase en el concepto de encargado del tratamiento que éste tratará los datos por cuenta del responsable del tratamiento o del responsable del fichero. Por lo tanto, en el caso español se prevé que el encargado actúe por cuenta de dos tipos de responsables.

En cuanto a la pluralidad de encargados del tratamiento hay que indicar, que en la legislación española, se ha regulado la posibilidad de subcontratación (art. 21 RLOPD)[487].

En lo que se refiere al elemento funcional que caracterizaba al responsable, la decisión sobre la finalidad, el contenido y el uso del tratamiento, ya he indicado que debería interpretarse de acuerdo con lo indicado por el GA29. Según el análisis que realizaba el GA29 lo que calificaba verdaderamente al responsable era el poder de determinación sobre los fines y lo que consideraba medios esenciales. Entre los medios esenciales no se encontraban las medidas técnicas, aunque el GA29 hacía referencia a que en ciertas legislaciones las decisiones respecto a las medidas de seguridad se consideran un aspecto esencial.

Entiendo que una de estas legislaciones es la española que ha desarrollado el principio de seguridad establecido en su artículo 9 LOPD mediante el RLOPD y que especifica en el artículo 12.2 LOPD que estas medidas deben incluirse en el contrato suscrito con el encargado del tratamiento. Si el encargado decidiera sobre la finalidad del tratamiento y los medios esenciales que incluirán las medidas de seguridad, deberá considerarse que no es un encargado y se le deberá aplicar el régimen general de la cesión.

---

administrativo) (ROJ: SAN 5137/2002), FJ 2 y SAN de 16 de julio de 2009 (Sala de lo contencioso-administrativo) (ROJ: SAN 3789/2009), FJ 6. En este mismo sentido, M. VIZCAÍNO CALDERÓN, *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Madrid, 2001, pág. 179 y R. GARCÍA DEL POYO VIZCAYA, "Encargado del tratamiento", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit*., pág. 1.088.

[487] Ver Capítulo VI.

Como se verá cuando se analicen los retos que supone la evolución tecnológica se han desarrollado modelos de negocio en los que se plantea un desequilibrio en la tradicional relación entre el responsable y el encargado, de forma que parece ponerse en peligro la capacidad de decisión del responsable[488]. Los clientes de este tipo de servicios de naturaleza eminentemente tecnológica tendrán dificultades para poder decidir sobre los medios del tratamiento cuando están frente a grandes empresas que fundamentan su negocio en bajos costes y en condiciones generales de contratación que no permiten margen de maniobra a quienes se suponen responsables.

b. La distinción entre responsable y encargado del tratamiento

Una de las cuestiones que, en la práctica, es más compleja en materia de protección de datos, es la delimitación entre responsable y encargado del tratamiento. Aparentemente los conceptos se distinguen claramente pero no siempre resulta tan fácil determinar cuando un sujeto actúa por cuenta de otro o si tiene esa capacidad de decidir que activaría su papel de responsable. Las consecuencias de errar en la calificación son importantes, ya que comportará el incumplimiento de lo establecido en la normativa. Además de lo señalado cuando se analizó la Directiva 95/46/CE, quiero apuntar algunos criterios aportados por la normativa y la doctrina españolas.

i. El criterio del nuevo vínculo

Una importante aportación del RLOPD es la fijación de un criterio utilizado para poder determinar si el sujeto es responsable o encargado: "se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado" (art. 20.1 RLOPD). Cuando entre el afectado, titular de los datos que el responsable transmita a un tercero, y ese tercero, se cree un nuevo vínculo jurídico, esto implicará que se esté ante una comunicación de datos. Por lo tanto, ese tercero no podrá ser considerado encargado del tratamiento. Este criterio proviene de algunos pronunciamientos judiciales de la Audiencia Nacional[489].

[488] Ver Capítulo VIII.

[489] SAN de 13 de septiembre de 2002 (Sala de lo contencioso-administrativo) (ROJ: SAN 4954/2002), FJ 5. En este asunto, una compañía de seguros había contratado a otra empresa la emisión de unas tarjetas para sus clientes que incluían el servicio de repostar combustible, servicio al que se dedicaba esta empresa que asumió el riesgo de las tarjetas. Una de las tarjetas que se emitió a una clienta de la compañía de seguros se

Como muestra de este criterio, en la prestación de servicios públicos se ha considerado que cuando la empresa contratada factura en su propio nombre existiría este nuevo vínculo[490]. No obstante, debe examinarse la relación que la empresa contratada tiene con el usuario para llevar a cabo este servicio, ya que, en ocasiones, mantiene una relación directa que es fruto del encargo, sin que pueda calificarse esta relación de nuevo vínculo jurídico.

No obstante, la inclusión de este criterio lo que hace es contribuir a la confusión. El hecho de que exista un nuevo vínculo jurídico entre encargado y afectado puede parecer que origina la imposibilidad de calificar al tratador efectivo como encargado. Sin embargo, la existencia de este vínculo sería un rasgo que denotaría que el sujeto, que se pretendía calificar de encargado, en realidad, debe calificarse como responsable porque tiene el poder de decidir sobre la finalidad, contenido y uso del tratamiento.

Estimo que la introducción de este criterio debería haberse orientado a aclarar que la existencia de este vínculo jurídico es muestra de que el encargado tiene este poder de decidir y no como un criterio para aplicar el régimen general de comunicación de datos desligado de los conceptos de encargado y responsable. De esta forma se hubiera adoptado una regulación más consistente en vez de socavar la fuerza de las definiciones.

---

envió por error en la consignación de la dirección por la clienta a otra persona que realizó un uso de la tarjeta que se cargó a la clienta. La empresa emisora de las tarjetas alegó que estaba amparada por el artículo 27 LORTAD, antecedente del artículo 12 LOPD, ya que había realizado un tratamiento por cuenta de la compañía de seguros. La Audiencia Nacional rechaza esta interpretación y entiende que, si bien para el servicio de emisión de tarjetas sí podía considerarse a esta empresa bajo el artículo 27 LORTAD, además se crea un nuevo vínculo jurídico entre esta empresa y los clientes de la compañía aseguradora, ya que es esta empresa la que podía reclamar el importe debido a la clienta, sin que esta clienta hubiera otorgado consentimiento ni fuera consciente de haber contraído relación alguna con esta empresa. A esta clienta se le emitió una tarjeta con un servicio de gasolina que ella no había solicitado y con unos datos que ella había proporcionado para otra finalidad, que era la de suscribir una póliza de seguro.

[490] Parece que sobre este criterio están de acuerdo la AEPD en su Informe 541/2008, A. TRONCOSO REIGADA, "La huida de la administración pública hacia el Derecho Privado y la privatización de los servicios públicos: consecuencias en el régimen jurídico de los ficheros de datos personales y en la delimitación del responsable y del encargado del tratamiento." *Anuario de la Facultad de Derecho de Alcalá de Henares, op. cit.,* págs. 57 a 66 y S. FARRÉ TOUS, "El encargado del tratamiento en el ámbito de las administraciones públicas", A. TRONCOSO REIGADA, A. (Dir.). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.,* pág. 1.109.

ii. La extensión de la legitimación del responsable: la doctrina de los datos adicionales

Otro ejemplo de criterio que sirve para determinar cuando estamos ante un encargado del tratamiento o no y que además enlaza con la extensión de la legitimación del tratamiento es la doctrina de los datos adicionales. Esta doctrina se ha elaborado en el contexto de las empresas de gestión de recobro de deudas. El supuesto que se planteaba era si una empresa que realizaba la gestión de recobro de deudas para sus clientes podía actualizar los datos personales que estas empresas le transmitían de los deudores, por ejemplo, el domicilio y el teléfono de contacto.

La Audiencia Nacional consideró que la empresa de gestión de recobro es encargada del tratamiento y actúa por cuenta de sus clientes. La legitimación para realizar el tratamiento que tiene el responsable se extiende al encargado mientras se limite a los datos que el responsable le proporcione del deudor, lo que no obsta para que el encargado pueda actualizarlos[491]. Además esa actualización deviene obligatoria en virtud del principio de calidad (art. 4 LOPD). En consecuencia, si el encargado decidiera tratar datos adicionales a los proporcionados por el responsable, debería considerarse que no se cumple con el encargo. El encargado decidiría sobre el contenido del tratamiento lo que le convertiría en responsable.

Este criterio sí que se conecta con el concepto, ya que lo que refleja es que el encargado decide sobre un aspecto que es claramente esencial, como es el contenido del tratamiento. Por otro lado, un rasgo muy importante para determinar cuando estamos ante un encargado del tratamiento es la extensión de la legitimación del responsable. De esta forma, siempre que podamos enmarcar la prestación de servicios del encargado en este

[491] Como indicaba la Audiencia Nacional "el consentimiento inicialmente prestado para el tratamiento de unos concretos datos personales –un domicilio determinado y un número de teléfono- continúa proyectándose en el tiempo mientras permanece la relación contractual respecto de datos personales del mismo tipo que los que fueron proporcionados y autorizado su uso siempre que su tratamiento continúe siendo necesario para el cumplimiento o ejecución del contrato, como aquí ocurre.(…) Como es evidente, ASINCO, que actúa como encargada del tratamiento, realiza su actividad para el cumplimiento del contrato de préstamo suscrito entre el señor Pedro Enrique y la Caja de Ahorros de Canarias y este contrato exige para su cumplimiento el tratamiento de los datos personales del domicilio y del número de teléfono de dicho señor para poder comunicar con él, especialmente cuando se constituye en mora y deja de cumplir con sus obligaciones, siendo indiferente a estos efectos que los concretos datos de domicilio y número de teléfono hayan cambiado pues su tratamiento está amparado en el consentimiento inicial o, en todo caso, en la excepción contenida en el art. 6.2 de la LOPD." SAN de 22 de julio de 2010 (Sala de lo contencioso-administrativo) (ROJ: SAN 3604/2010), FJ 5º y SAN de 21 de enero de 2010 (Sala de lo contencioso-administrativo) (ROJ: SAN 438/2010), FJ 5º, que remiten a la sentencia de 14 de mayo de 2009. Recoge esta doctrina la AEPD en su informe 112/2012.

supuesto de legitimación, estaremos ante un encargo. La AEPD ha señalado también que el tratamiento no debería reportar al encargado otro beneficio que el derivado de la prestación de servicios propiamente dicho[492]. Y es que si el encargado obtiene otro beneficio es porque llevará a cabo una extralimitación del encargo seguramente.

iii. Legislación, relación contractual e influencia de hecho

Además de los criterios apuntados, para identificar si un sujeto es responsable o encargado se podrá acudir también a los criterios que se expusieron en el análisis del concepto de responsable, en la Directiva 95/46/CE. Y es que si se busca la fuente de la que procede el poder de decisión, sea una competencia legal explícita, implícita o derivada de una influencia de hecho, respecto al tratamiento esto ayudará a identificar quién ejerce este poder y quién no. Asimismo, como también se indicó en el estudio del concepto de encargado en la Directiva 95/46/CE nada obsta para que se pueda calificar al mismo en la legislación. En la normativa española se pueden encontrar algunos ejemplos que sirven para ilustrar lo limitado de esta opción.

Así, uno de estos ejemplos es la Ley de contratos del sector público que establece que, en el caso de que la contratación implicara que el contratista accediera a datos de carácter personal de cuyo tratamiento fuera responsable la entidad contratante, aquél tendría la consideración de encargado del tratamiento[493]. No obstante, ¿esto implica que en todos los casos en que haya una contratación en el marco del sector público y que implique el acceso a datos personales la entidad contratista será encargada del tratamiento? La respuesta debe ser negativa y habrá que estar al caso concreto, especialmente en los contratos que tienen como objeto la prestación de servicios públicos donde no puede establecerse de forma automática esta calificación[494].

[492] Informe 309/2008 de la AEPD.
[493] Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la ley de contratos del sector público, (BOE núm. 276 de 16.11.2011), Disposición adicional vigésima sexta. Además esta disposición contiene una regulación que viene a reproducir la que se establece en la LOPD y en el RLOPD sobre el encargo del tratamiento.
[494] Como afirma TRONCOSO que realiza un estudio de esta cuestión debe estarse al caso concreto. A. TRONCOSO REIGADA, "La huida de la administración pública hacia el Derecho Privado y la privatización de los servicios públicos: consecuencias en el régimen jurídico de los ficheros de datos personales y en la delimitación del responsable y del encargado del tratamiento." *Anuario de la Facultad de Derecho de Alcalá de Henares, op. cit.,* págs. 67 a 68.

De esta forma, de los informes de las autoridades de protección datos se puede ver que se acude a diversos aspectos para determinar si la entidad contratista es encargada del tratamiento o responsable y que no son todo lo clarificadores que debieran[495] aunque parece que hay una tendencia hacia un análisis más matizado[496]. Es importante que el análisis se centre en si efectivamente existe el poder de decisión. Si se intenta acudir a otros aspectos más objetivos, como en quien radica la competencia o quien asume el riesgo económico, al final lo que se origina es una interpretación confusa de los supuestos y una dificultad mayor para los responsables al aplicar la normativa[497]. Esta consecuencia

[495] Así, en su Informe 541/2008 la AEPD debía determinar si una entidad adjudicataria de un servicio de suministro de agua debía considerarse encargado del tratamiento. La AEPD remitía al artículo 251.1 de la Ley 30/2007, de 30 de octubre, de contratos del sector público (actual artículo 275.1 del vigente Real Decreto Legislativo 3/2011) que establecía: "La Administración podrá gestionar indirectamente, mediante contrato, los servicios de su competencia, siempre que sean susceptibles de explotación por particulares. En ningún caso podrán prestarse por gestión indirecta los servicios que impliquen ejercicio de la autoridad inherente a los poderes públicos." La AEPD consideraba que si el objeto del contrato conllevara la recaudación de tasas municipales esto estaría ligado a la labor recaudatoria y la entidad adjudicataria sería un encargado del tratamiento. Respecto a este argumento, se pronuncia en contra FARRE TOUS, ya que considera que la calificación de encargado no se puede ver alterada por la remuneración que pueda percibir. S. FARRÉ TOUS, "El encargado del tratamiento en el ámbito de las administraciones públicas", A. TRONCOSO REIGADA, A. (Dir.). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, págs. 1.109 a 1.110. La ACPD, en referencia a supuestos de concesión del servicio de suministro de agua potable de ayuntamientos, en un dictamen de 2006 estimó que la empresa privada que prestaba este servicio debía ser considerada encargada del tratamiento. La ACPD entendía que el ayuntamiento era responsable de acuerdo con la normativa de régimen local de la prestación de este servicio que consideraba un servicio básico. Dictámen CNS-10/2006 de la ACPD.

[496] Así la AEPD, en su Informe 267/2010, que reproducía el contenido de un informe de 5 de noviembre de 2002, se refería a la delegación de los ayuntamientos a las diputaciones provinciales de las facultades de gestión, liquidación, inspección y recaudación tributarias. Pues bien, la AEPD esta vez introduce más matizaciones a lo indicado previamente en el informe comentado (Informe 541/2008). Así indicaba que en estos casos no se podía decir en abstracto si la encomienda llevaba aparejada una relación de responsable y encargado o si se trataba de una cesión de datos entre dos responsables. La AEPD argumentaba que si la actividad de la administración a la que se delegaban las competencias se limitaba a la recepción de los datos, la realización de las actividades necesarias para llevar a cabo el servicio y posteriormente restituía al titular de la competencia la información facilitada, estaríamos ante un encargado del tratamiento. En cambio, si la administración a quien se encomendara la gestión tributaria por parte de varias administraciones procediera a la creación de tratamientos específicos que supusieran la organización interna de los datos, de forma que fuera la propia administración delegada la que decidiera sobre el tratamiento, su contenido y los usos que deberían darse a los mismos (como sucedería si dicha aplicación pudiera ser objeto de consulta por parte de otros órganos de la administración), la administración delegada sería responsable de un nuevo tratamiento. Respecto a la ACPD, en un dictamen de 2013, también matiza lo indicado en su Dictámen CNS-10/2006 en un supuesto de concesión del servicio de suministro de agua. Si bien el ayuntamiento será responsable último de la información derivada del servicio, puede articularse la responsabilidad de varias formas. El ayuntamiento puede ser responsable del fichero y la entidad concesionaria encargada del tratamiento o puede establecerse que la responsabilidad del fichero recaiga en la entidad concesionaria. Dictámen CNS-28/2013 de la ACPD.

[497] Así TRONCOSO REIGADA y FARRÉ TOUS están de acuerdo en rechazar como argumento para determinar la responsabilidad en un servicio público la asunción del riesgo económico. TRONCOSO REIGADA señala que el primer criterio debe ser quién decide sobre la finalidad del tratamiento, su contenido y su uso, es decir, aplicar el concepto de responsable. También indica que si la empresa privada decide tratar los datos para finalidades propias sería responsable. Como aspectos que denotan quién es el responsable también señala en nombre de quien se realice la recogida de datos personales, la apariencia externa que percibe el titular de los datos y lo que recojan los pliegos de contratación. Resulta interesante también los criterios que, según TRONCOSO REIGADA, no son útiles para esta determinación. Así,

tiene especial relevancia en este sector porque puede suponer la aplicación de una regulación diferente, según se trate de ficheros de titularidad privada o pública. Si el contratista es una empresa privada y se califica de responsable, el régimen aplicable será el de los ficheros de titularidad privada. En cambio, si se le considera un encargado del tratamiento, deberá estarse a la regulación de los ficheros de titularidad pública.

Otro aspecto a tener en cuenta en la legislación española es que no se ha previsto la vía de escape que establece la Directiva 95/46/CE que permite tratar los datos al encargado para cumplir con un imperativo legal (art. 16 Directiva 95/46/CE). No obstante, debería entenderse que cabe aplicar esta excepción aunque no esté prevista. Así lo ha entendido la ACPD en una de sus recomendaciones, en la que además incentiva el proceso de reflexión acerca del modelo a elegir por el responsable en la contratación[498].

Si bien la legislación será una fuente para poder determinar si estamos ante un responsable o un encargado, en el ordenamiento español tiene especial relevancia el análisis de la relación contractual que exista entre responsable y encargado, lo que respondería a la capacidad de influencia de hecho. Y es que se ha incidido especialmente en el contrato como requisito para poder aplicar la regulación del encargado del tratamiento, ya que se configura la misma como una excepción a la regulación general de la cesión de datos.

Independientemente de que se revise el contrato para poder aplicar este régimen excepcional, también servirá para determinar quién es el responsable y quién es el

además del criterio del riesgo económico apuntado, para este autor no se debe valorar a quién corresponde la competencia administrativa, ya que siempre daría como resultado que el responsable es la administración contratante. Únicamente le parece útil este criterio cuando se intente determinar quién es responsable entre diferentes administraciones públicas. Tampoco se deben utilizar como criterios, según el autor, para atribuir responsabilidad la titularidad del servicio público ni el sometimiento por parte de la empresa privada a un régimen de autorización administrativa, o a una determinada normativa administrativa, o que reciba ayudas o subvenciones ni que se ostenten potestades de inspección sobre esta empresa privada ni que la administración fije las tarifas del servicio o que realice un control de calidad sobre esta empresa. A. TRONCOSO REIGADA, "La huida de la administración pública hacia el Derecho Privado y la privatización de los servicios públicos: consecuencias en el régimen jurídico de los ficheros de datos personales y en la delimitación del responsable y del encargado del tratamiento." *Anuario de la Facultad de Derecho de Alcalá de Henares, op. cit.*, págs. 57 a 66. S. FARRÉ TOUS, "El encargado del tratamiento en el ámbito de las administraciones públicas", A. TRONCOSO REIGADA, A. (Dir.). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, pág. 1.109.

[498] Recomendación 1/2010 de la *Agència Catalana de Protecció de Dades*, sobre el encargado de tratamiento en la prestación de servicios por cuenta de entidades del sector público de Cataluña, apdos. 5, 21.

encargado en esa concreta relación contractual. De nuevo, esto no significa que sólo deba estarse a lo establecido en el contrato, sino que lo que debe analizarse es el supuesto de hecho.

También se tienen en cuenta los otros criterios apuntados por el GA29 para resolver si existe la capacidad de influencia de hecho, como el grado de control real o las expectativas razonables o la imagen que puedan tener los titulares de los datos sobre quién tiene el poder de decisión que ha acogido el Tribunal Supremo[499].

[499] STS de 29 de junio de 2010 (Sala 3ª) (ROJ: STS 3674/2010), FJ 2.

PARTE II
EL RESPONSABLE COMO ELEMENTO CLAVE EN LA REGULACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS

Tras haber realizado el análisis del concepto de responsable en la legislación reguladora del derecho a la protección de datos, esta parte se dedicará al estudio de los tres aspectos que se han extraído de esta regulación en los que la figura se erige como elemento central. Estos tres aspectos son: la determinación de la legislación aplicable, el cumplimiento de las obligaciones establecidas en la normativa y la atribución de responsabilidades.

CAPÍTULO IV
EL RESPONSABLE COMO CRITERIO DE DETERMINACIÓN DE LA LEGISLACIÓN APLICABLE

Una de las preocupaciones del legislador en una norma como la Directiva 95/46/CE de alcance supranacional es la previsión de criterios que puedan servir para determinar la legislación aplicable en caso de conflicto. La transposición de estos criterios debería servir para armonizar las reglas que aplicarán los Estados miembros en estos supuestos. Como veremos, de nuevo asistimos a la existencia de divergencias en esta traslación de los criterios al ámbito nacional.

Cuando se elaboró la Directiva 95/46/CE se tuvo en cuenta ya la necesidad de dar alcance a responsables que se ubicaran fuera de la UE y la dificultad de hacerlo en un entorno tecnológico en el que las fronteras territoriales existentes, sólo permanecen en el mundo *offline*. Precisamente, esta dificultad hizo que, durante la elaboración del Convenio 108 se tuviera que abandonar el debate sobre la ley aplicable por el miedo a bloquear la aprobación del texto por los Estados parte[500].

En el proceso legislativo de la Directiva 95/46/CE se pasó, en un primer momento, del criterio de la ubicación del fichero al del establecimiento del responsable del tratamiento para poder determinar la legislación aplicable. Ya en ese entonces, se

[500] Ver Capítulo I.

consideró que sería más fácil definir dónde se encontraba el establecimiento del responsable que verificar dónde se hallaba el fichero[501]. Por tanto, el concepto de responsable del tratamiento se convirtió en una cuestión clave también para resolver los conflictos sobre la ley aplicable. A continuación analizaré las reglas establecidas en la Directiva 95/46/CE y cómo se ha realizado su transposición en las leyes europeas nacionales[502].

1. TRATAMIENTO EFECTUADO EN EL MARCO DE LAS ACTIVIDADES DE UN ESTABLECIMIENTO DEL RESPONSABLE DEL TRATAMIENTO EN EL TERRITORIO DE UN ESTADO MIEMBRO: EL PRIMER CRITERIO

La regulación contenida en la Directiva 95/46/CE persigue el objetivo de evitar que una persona sea excluida de la protección que pretende garantizar esta norma, por lo que en su preámbulo parte de la premisa de que todo tratamiento de datos personales efectuado en la UE deberá respetar la legislación de uno de sus Estados miembros (Considerando 18 Directiva 95/46/CE)[503]. Si el tratamiento se produce en un Estado miembro no habrá conflicto y se aplicará la ley de este Estado. Sin embargo, si surge un conflicto de leyes en el ámbito de la UE se establece un primer criterio:

[501] Dictamen 8/2010 sobre el derecho aplicable, 0836-02/10/ES, WP 179, 16.12.2010, Grupo de trabajo Artículo 29 sobre la protección de datos, pág. 8. También M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, pág. 91.

[502] Estas divergencias existentes en las leyes nacionales fueron apuntadas ya en varios estudios de la aplicación de la Directiva 95/46/CE, entre los que destaco el estudio realizado con ocasión del proceso de reforma de la directiva: *Commission Staff Working Paper, Impact assessment accompanying the document Regulation of the European Parliament […], op. cit., Annex 2*, págs. 23 y 25. Este estudio remite al Informe de la Comisión sobre la aplicación de la Directiva sobre protección de datos (95/46/CE), COM(2003) 265 final, Bruselas, 15.5.2003, en el que ya se llamó la atención sobre la deficiente transposición del artículo 4 de la Directiva 95/46/CE, de forma que los conflictos que se pretendían evitar, se incrementaron. En el estudio de 2012 se indica que no se ha mejorado la situación desde el año 2003. El hecho de enlazar la ley aplicable con el establecimiento del responsable del tratamiento lo que hace es que un mismo responsable deba cumplir las legislaciones de los diversos Estados miembros que contemplan requisitos divergentes y destaca también la dificultad de saber la ley aplicable en el entorno de Internet.

[503] Los Considerandos 18 a 21 Directiva 95/46/CE sirven para explicar el alcance del artículo 4, al que se llegó tras un proceso de elaboración complicado que tuvo que enfrentarse a bastantes obstáculos. De esta forma, según indica HEREDERO HIGUERAS, el Considerando 18 sienta la regla de que un tratamiento de datos que se efectúe en la UE debe respetar la legislación de un Estado miembro. Los demás considerandos precisan cómo llegar a determinar esa legislación de forma que se eviten en lo posible prácticas de *forum shopping*. El Considerando 21 ("Considerando que la presente Directiva no afecta a las normas de territorialidad aplicables en materia penal") es la respuesta a los problemas de territorialidad del derecho penal o sancionador, ya que en caso de delito o infracción administrativa cometidos respecto a un tratamiento en el territorio de un Estado miembro diferente a aquel en el que el responsable del tratamiento estuviera establecido, no podría aplicarse la legislación del establecimiento de este responsable al regir la legislación del lugar de comisión. M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, págs. 92 a 95.

> "Los Estados miembros aplicarán las disposiciones nacionales que hayan aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable;" (art. 4.1.a) de la Directiva 95/46/CE).

Este criterio gira en torno al tratamiento de datos, pieza esencial en la Directiva 95/46/CE. Sin embargo, no se acude al lugar donde se realiza el tratamiento, sino al lugar donde se halla ubicado un establecimiento del responsable del tratamiento. El tratamiento de datos podrá efectuarse en un Estado miembro diferente de aquel donde el responsable tenga su establecimiento o incluso fuera del EEE y, de todas formas, la legislación aplicable podrá ser la del Estado miembro donde se ubique el establecimiento de ese responsable. Por tanto, el ámbito de aplicación de la Directiva 95/46/CE es extraterritorial[504].

1.1. La noción del establecimiento

La Directiva 95/46/CE especifica "*un* establecimiento", por lo que se deduce que no debe tratarse del establecimiento principal del responsable del tratamiento, sino que podrá tratarse de cualquier tipo de establecimiento. Además, si hay varios establecimientos en varios Estados miembros, podrán originar la aplicación de diferentes leyes a establecimientos del mismo responsable. Por ello, el GA29 alude a una aplicación más distributiva que uniforme del derecho nacional en caso de múltiples establecimientos[505].

Respecto a la noción de establecimiento, éste debe implicar el ejercicio efectivo y real de una actividad mediante una instalación estable (Considerando 19 Directiva 95/46/CE)[506]. La forma jurídica de dicho establecimiento no es un factor determinante al

[504] Dictamen 8/2010 sobre el derecho aplicable, *op. cit.*, pág. 10.
[505] *Ibídem*, pág. 9.
[506] El GA29 alude a la posible utilización de la interpretación realizada por el TJUE respecto de la libertad de establecimiento de conformidad con el artículo 50 TFUE, que hace referencia a una "integración permanente de medios humanos y técnicos necesarios para las prestaciones de determinados servicios". Sentencia del TJUE de 4 de julio de 1985, *Gunter Berkholz*, C-168/84, EU:C:1985:299 y Sentencia del TJUE de 7 de mayo de 1998, *Lease Plan Luxembourg SA*, C-390/96, EU:C:1998:206, *Ibídem*, pág. 13. En

respecto. El GA29 cita algunos ejemplos de lo que considera establecimiento, como un bufete de abogados o una oficina de una persona, en la medida en que haga algo más que representar al responsable del tratamiento[507]. No sería establecimiento, según el GA29, un servidor u ordenador ya que los considera más una herramienta. También en las leyes que transponen la Directiva 95/46/CE se encuentran desarrollos de lo que consideran establecimiento, como en las Leyes irlandesa, inglesa o austríaca[508].

Sin embargo, hay que tener presente que este primer criterio, como ya se ha apuntado, no se limita a la existencia de un establecimiento del responsable del tratamiento, sino que especifica que es necesario que el tratamiento sea efectuado en el marco de las actividades de este establecimiento. Por tanto, habrá que analizar el tratamiento y si hay varios establecimientos identificar qué hacen concretamente respecto al mismo cada uno de ellos. Este matiz es el que otorga cierta dificultad a la aplicación del criterio, complejidad y matiz que pocas de las leyes nacionales han transpuesto correctamente[509].

---

la legislación española se reproduce el contenido de este Considerando 19 en el artículo 3.2 RLOPD: "[…] se entenderá por establecimiento, con independencia de su forma jurídica, cualquier instalación estable que permita el ejercicio efectivo y real de una actividad."

[507] Dictamen 8/2010 sobre el derecho aplicable, *op. cit.*, págs. 13 a 14.

[508] De esta forma, la Ley irlandesa indica ejemplos de lo que se considerará establecimiento: "un individuo residente en el Estado, compañías, asociaciones que se creen de acuerdo con la normativa nacional, personas que mantengan en el Estado oficina, filiales, agencias a través de las que lleve a cabo una actividad o personas que mantengan en el Estado una práctica habitual" (art. 1.3.B.b) Ley irlandesa). También la Ley inglesa especifica lo que se entiende por responsable establecido en el Reino Unido: "un individuo residente habitualmente en Reino Unido; una sociedad creada de acuerdo con el derecho del Reino Unido; un partenariado u otra asociación no configurada como sociedad creada de acuerdo con el derecho del Reino Unido; cualquier persona que no se encuentre en los supuestos anteriores pero que mantenga en el Reino Unido: (i)una oficina, filial o agencia a través de la que lleve a cabo su actividad o (ii)su práctica habitual" (art. 5.3 Ley inglesa*).* La Ley austríaca establece asimismo una definición de lo que considera establecimiento que describe como "cualquier unidad organizativa constituida de forma autónoma en términos de disposición y funciones por instalaciones fijas en un lugar determinado, con o sin estatus de persona jurídica, que lleva a cabo actividades en el lugar donde se encuentra" (parágrafo 4.15 Ley austríaca).

[509] Principalmente las leyes se limitan a disponer que se aplique la ley cuando el responsable del tratamiento esté establecido en el territorio del Estado miembro (art. 1.5 *a sensu* contrario Ley alemana; art. 3.3.a) Ley chipriota; art. 5 Ley eslovena; art. 4.1 Ley finlandesa; art. 5.1 Ley francesa; art. 3.a) Ley griega; art. 5.1 Ley italiana; art. 3.1 Ley letona; art. 3.2.a) Ley luxemburguesa; sección 4 Ley noruega; art. 3.2 Ley polaca; sección 4 Ley sueca). Otras van un poco más allá sin llegar a recoger la referencia completa, como la Ley inglesa que se refiere a "en el marco de un establecimiento" (art. 5.1.a Ley inglesa); la Ley irlandesa que se refiere a "en el contexto de un establecimiento"(art. 1.3b Ley irlandesa); la ley de Liechtenstein que se aplica al tratamiento de datos que se lleve a cabo como parte de las actividades de una filial del responsable de fichero en Liechtenstein (art. 2.2.a) Ley de Liechtenstein). Algunas leyes no se refieren ni siquiera al establecimiento del responsable, como la Ley austríaca que establece que se aplicará cuando el uso de los datos se efectúe en Austria (art. 1 Ley austríaca) y la Ley húngara que indica que se aplicará a las actividades de tratamiento y de control de datos que se lleven a cabo en Hungría (sección 2.1 Ley húngara). La Ley croata no transpone los criterios del artículo 4 Directiva 95/46/CE y se limita a indicar que la ley se aplica a la protección de datos de personas físicas y la supervisión de la recogida, tratamiento y uso de los

Como ejemplo cabe citar la ley española, la LOPD, que, al recoger este primer criterio no lo hizo exactamente igual, de forma que se modificó el significado del precepto: "se regirá por la presente ley orgánica todo tratamiento de datos de carácter personal cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento" (art. 2.1.a) LOPD). Como puede observarse, el criterio cambia radicalmente, ya que se exige que el tratamiento esté ubicado en España. Por eso, se quiso corregir esta disposición mediante la aprobación del RLOPD que reprodujo literalmente el criterio de la Directiva 95/46/CE[510].

También, hay que tener en cuenta que un tratamiento de datos consta de diferentes fases y operaciones, lo que resulta en que podrían ser aplicables al mismo tratamiento diferentes leyes, debido a que las diferentes etapas en las que puede dividirse un tratamiento podrían realizarse en el marco de diferentes establecimientos ubicados en diferentes Estados miembros. No obstante, el GA29 señala que debe tenerse una visión global de las actividades del tratamiento, de forma que si una serie de operaciones realizadas en distintos Estados miembros están orientadas hacia un único propósito podrían llevar a la aplicación de una sola ley nacional[511].

---

datos personales en la República de Croacia (art. 1 Ley croata). No transpone este primer criterio la Ley estonia ni la Ley checa. Sí se aproximan al criterio de la Directiva 95/46/CE la Ley belga que alude a que el tratamiento se efectúe en el marco de las actividades reales y efectivas de un establecimiento fijo del responsable del tratamiento sobre el territorio belga (art. 3bis Ley belga); la Ley búlgara que indica que se aplicará al responsable del tratamiento establecido en el territorio de la República de Bulgaria que trate datos personales en conexión con su actividad en el país (art. 1.4 Ley búlgara); la Ley danesa que establece que será aplicable al tratamiento de datos que se lleve a cabo por cuenta del responsable que esté establecido en Dinamarca y las actividades se lleven a cabo en el territorio de la Unión Europea (art. 4 Ley danesa); la Ley lituana que se aplicará si el tratamiento de datos lo realiza un responsable establecido y que opera en el territorio de Lituania, en el marco de sus actividades (art. 1.3.1 Ley lituana); la Ley rumana se aplica si el tratamiento se lleva a cabo en el marco de las actividades de los responsables establecidos en Rumanía (art. 2.2.a Ley rumana); la Ley islandesa se aplica a los tratamientos de datos que se realicen en nombre de un responsable establecido en Islandia, si el tratamiento se lleva a cabo en el EEE o en un país o un lugar que la autoridad de control incluya en una lista en el boletín oficial (art. 6 Ley islandesa). Transponen fielmente este primer criterio la Países Bajos (art. 4.1 Ley Países Bajos), Malta (art. 4.1.a Ley maltesa), Portugal (art. 4.3.a Ley portuguesa).

[510] De esta forma, la AEPD, cuando debe recurrir a este criterio, obvia el artículo 2.1.a) LOPD y acude al artículo 3.1.a) RLOPD donde se reprodujo el criterio. J. APARICIO SALOM, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, 4ª Ed., Aranzadi, Cizur Menor (Navarra), 2013, pág. 40. Así lo explica la AEPD en su Resolución R/02892/2013 de 18 de diciembre de 2013, en Procedimiento nº PS/00345/2013, FJ V.

[511] Dictamen 8/2010 sobre el derecho aplicable, *op. cit.*, pág. 15. SANCHO VILLA indica que si parte del tratamiento se produce en un establecimiento del responsable en un Estado del EEE y parte en otro, debería aplicarse cada una de las leyes implicadas cuando los tratamientos son operaciones individualizadas, de acuerdo con el principio de aplicación distributiva deducido de la directiva. También considera esta autora

Para desentrañar lo que implica la expresión "en el marco de las actividades" el GA29 alude a varios aspectos que se tendrán en cuenta[512]. El primer aspecto sería el grado de implicación del establecimiento en las actividades en cuyo marco se traten los datos personales, lo que en la práctica equivale a contestar a la pregunta "quién hace qué" ¿Qué actividades efectúa cada establecimiento? Si un establecimiento trata datos para llevar a cabo sus actividades, sería la ley de este establecimiento la que se tendría que aplicar. Si un establecimiento trata datos personales en el marco de actividades de otro establecimiento, será la ley de ese otro establecimiento la que deberá aplicarse.

El segundo aspecto que cita el GA29 es el relativo a la naturaleza de las actividades del establecimiento. Sin embargo, esta característica se considera un elemento secundario que puede ayudar a definir la ley aplicable. Un ejemplo que cita el GA29 y que es habitual en la práctica de las empresas multinacionales es la centralización de la base de datos de recursos humanos[513].

De esta forma, si la base de datos de recursos humanos de una multinacional se ubica en un establecimiento que se halla en el Reino Unido y a la misma se transfieren los datos personales de los empleados de las diversas filiales, como puede ser la irlandesa, la ley aplicable en el caso de los datos personales de los empleados de la filial irlandesa sería la irlandesa porque el establecimiento, en el marco del que se lleva a cabo el tratamiento, sería la filial irlandesa en virtud de su papel de empleador. De esta forma, como indica el GA29, deberían aplicarse leyes de diferentes países a esta base de datos.

Lo importante, en este caso, será determinar si las actividades en función de las que se realiza el tratamiento son de un establecimiento o del otro. Si se trata de una actividad que realiza un primer establecimiento, pero que temporalmente decide que lo

---

un argumento para apoyar esta aplicación el concepto tan amplio de tratamiento que incluye la Directiva 95/46/CE. Además esta interpretación también, según la autora, permite no tener que pronunciarse sobre elementos que podrían complicar el análisis como el carácter accesorio o instrumental de un tratamiento respecto a otro. D. SANCHO VILLA, "Ámbito de aplicación territorial", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, pág. 103.

[512] Dictamen 8/2010 sobre el derecho aplicable, *op. cit.*, pág. 16.

[513] *Ibídem*, pág.18 (ejemplo nº 4).

lleve a cabo otro establecimiento con sus instrucciones, se aplicará la ley del primer establecimiento.

Esta interpretación que sigue los criterios del GA29, al final puede llevar también al *forum shopping* si las normativas no están debidamente armonizadas, ya que el reparto de actividades entre los diferentes establecimientos del responsable del tratamiento podría acomodarse para facilitar la aplicación de las leyes más favorables al responsable.

Por eso, al igual que sucede con el análisis del concepto del responsable del tratamiento, debería atenderse al supuesto de hecho para ver realmente el establecimiento que debería activar la aplicación de la ley. De hecho, lo más conveniente sería aplicar los mismos criterios que se aplican en el concepto del responsable del tratamiento, de forma que el establecimiento que decida sobre los fines y los medios del tratamiento debería desencadenar la ley aplicable.

Y es que, pese a que aparentemente los criterios que proporciona el GA29 para determinar cuándo se estará ante un tratamiento de datos efectuado en el marco de las actividades de un establecimiento del responsable, son específicos para esta situación, el análisis que se realiza, al final nos lleva por la misma senda que el análisis de identificación de un responsable del tratamiento.

De esta forma, si las actividades de un establecimiento, como puede ser la filial irlandesa en el ejemplo de la base de datos de recursos humanos centralizada, implican que deba realizar un tratamiento de datos personales, será este establecimiento el que deberá activar la ley aplicable. En cierta manera se determinaría a este establecimiento como el que debería determinar los fines y medios del tratamiento, porque sería el establecimiento “responsable del tratamiento”. Si este tratamiento de datos, que está ligado a las actividades del establecimiento de la filial irlandesa, se decide, por un tema de gestión, que lo pase a realizar el establecimiento del Reino Unido, el tratamiento no deja de estar ligado a las actividades de la filial irlandesa. En consecuencia, el establecimiento del Reino Unido ejercería un rol similar al de un “encargado del tratamiento” del establecimiento irlandés y, por tanto, seguiría siendo aplicable la ley irlandesa.

Un enfoque que ayudaría a resolver esta cuestión de una forma más adecuada sería utilizar los criterios relativos a la diferenciación entre responsable y encargado del tratamiento para poder determinar la legislación aplicable a los diversos establecimientos del responsable del tratamiento. Sin embargo, esto limitará la utilidad del criterio, ya que si estos establecimientos pueden determinar los fines y los medios del tratamiento debería activarse su papel de responsable del tratamiento y no sería necesario acudir al criterio de ley aplicable.

1.2. ¿Nuevo responsable del tratamiento o establecimiento? Interpretación de la Directiva 95/46/CE versus leyes nacionales

¿Cómo se puede conjugar, entonces, la interpretación que realiza el GA29 relativa a la aplicación a un establecimiento de un responsable del tratamiento con la activación del concepto de responsable del tratamiento? El preámbulo de la Directiva 95/46/CE nos indica que un establecimiento es cualquier entidad, tenga o no personalidad jurídica y, concretamente menciona la filial y la sucursal como ejemplos de lo que se puede considerar establecimientos del responsable (Considerando 19 Directiva 95/46/CE).

Si se tiene en cuenta el análisis realizado al elemento subjetivo del concepto de responsable se puede recordar que, evidentemente podían ser responsables aquellos sujetos que tuvieran personalidad jurídica e incluso en algunas leyes se consideraba que también los entes sin personalidad jurídica podían ser responsables, como sucede precisamente en la legislación española[514]. Asimismo, en el momento en que un sujeto cumple con los elementos del concepto se convertirá en responsable del tratamiento, lo que significa que la legislación aplicable debería activarse respecto a los establecimientos de este responsable del tratamiento.

De nuevo nos enfrentamos a una dificultad en la aplicación de esta regulación. Por un lado, el GA29 ha perfilado una interpretación de este criterio, establecido en el artículo 4.1.a) Directiva 95/46/CE, en la que entiende que un responsable del tratamiento único puede tener una serie de establecimientos respecto a los que es necesario determinar qué legislación es aplicable. Por el otro, se estará ante la interpretación de las leyes nacionales

[514] Ver Capítulos II y III.

que, como en el caso de la legislación española, al entender que este establecimiento (una filial o una sucursal o cualquier otro ente, tenga o no personalidad jurídica) determina los fines y medios del tratamiento de datos personales concluye que está ante un nuevo responsable, que desencadena la aplicación de la ley (en este caso española)[515]. Por tanto, ya no sería necesario ver si se aplica el criterio que precisa para aplicar la ley que se esté ante un tratamiento efectuado en el marco de las actividades de un establecimiento.

El criterio, tal como lo expone el GA29, sólo tendría sentido si estuviéramos ante un sujeto que, de acuerdo con el concepto de responsable del tratamiento, no lo cualificara como tal responsable. Sin embargo, esto difícilmente permitirá considerar que se realice el tratamiento en el marco de las actividades de este establecimiento, ya que si no activa la calificación de responsable es porque no tendrá esa capacidad de determinación sobre el tratamiento.

Pues bien, esta cuestión se ha resuelto mediante la sentencia del TJUE en el asunto *Google*[516]. El TJUE consideró que *Google Inc.*, la matriz del grupo, y la empresa que gestionaba el motor de búsqueda de *Google*, debía ser considerada responsable del tratamiento respecto a los datos personales que el motor de búsqueda trataba. *Google Inc.* creó una filial en España, *Google Spain, S.L.* que se ocupaba de la venta de espacios publicitarios en el buscador. Pues bien, el TJUE estimó que debía aplicarse el criterio del artículo 4.1.a) Directiva 95/46/CE, al entender que *Google Spain, S.L.* era un establecimiento del responsable del tratamiento que se localizaba en territorio español y que el tratamiento de datos personales se realizaba en el marco de las actividades del mismo.

[515] Un ejemplo de esta interpretación es la realizada por la AEPD en respuesta a una consulta que se le planteaba precisamente sobre si se debía entender aplicable la ley española de protección de datos a una sucursal que había abierto una entidad ubicada fuera del territorio español. De esta forma se preguntaba a la AEPD si se le podía aplicar a esta sucursal lo dispuesto en el artículo 2.1 a) LOPD en conexión con el artículov4.1.a) Directiva 95/46/CE. Pues bien, pese a referirse la AEPD al criterio relativo al establecimiento, acude a la definición del responsable del fichero en el artículo 5.1.f) RLOPD que especifica que podrán ser responsables "los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados". Al entender que sobre la sucursal en cuestión se cumplen todos los elementos que debe reunir un responsable del fichero de acuerdo con la definición de la ley española, entiende que ésta debe calificarse de responsable y que debe cumplir con las obligaciones que establece la ley española. Informe jurídico de la AEPD 569/2008.

[516] Sentencia del TJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2014:317. Ver Capítulo VIII.

Sin duda, se trata de una interpretación forzada de la Directiva 95/46/CE, con el fin de ampliar su ámbito de aplicación para proteger a los ciudadanos europeos. Debido a su evidente trascendencia, se retomará más en profundidad el análisis de esta sentencia posteriormente, cuando se aborden los retos que el mundo digital ha supuesto para la figura del responsable[517]. No obstante, para mostrar la repercusión del pronunciamiento, se puede mencionar las actuaciones que, en el año 2015, llevó a cabo la autoridad de control belga contra la red social *Facebook*.

La autoridad belga emitió una recomendación dirigida a *Facebook*, a sus usuarios finales y a quienes utilizaban en sus sitios web los *plug-in* sociales de *Facebook*[518]. Este documento fue el resultado de un análisis de la nueva política de privacidad aprobada por *Facebook* que entró en vigor el 30 de enero de 2015 y el funcionamiento del mismo. Fundamentalmente se instaba a la red social a que modificara algunas de sus prácticas en materia de *cookies* y de *plug-in* sociales, ya que la autoridad consideraba que no cumplían con la legislación belga de protección de datos.

Sin embargo, lo que nos interesa es la argumentación utilizada por *Facebook* para eludir la aplicación de la Ley belga[519]. Esta red social tiene su matriz, *Facebook Inc*. establecida en EEUU pero había creado una sociedad en Bélgica, *sprl Facebook Belgium*. La autoridad de control belga se puso en contacto con esta sociedad belga, a lo que ésta respondió que la responsable del tratamiento de los datos de los usuarios belgas, así como del resto de la UE, era la sociedad irlandesa *Facebook Ireland Limited* que utilizaba a *Facebook Inc* y *sprl Facebook Belgium* como encargados del tratamiento. Así lo indicaba esta compañía en su política de privacidad y también había suscrito los oportunos contratos de encargo del tratamiento. Por tanto, *Facebook* sólo admitía como legislación aplicable la irlandesa.

La autoridad belga analiza el supuesto y acude a la documentación pública mercantil presentada por *Facebook* sobre la sociedad a las autoridades estadounidenses, así como a información mercantil de la sociedad belga. De esta forma, la autoridad

[517] Ver Capítulo VIII.
[518] *Recommandation nº 04/2015 du 13 mai 2015, Comission de la protection de la vie privée,* http://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_04_2015.pdf (fecha consulta: 8.7.2015).
[519] *Recommandation nº 04/2015 du 13 mai 2015, Comission de la protection de la vie privée, op. cit.,* págs. 4 a 6.

argumenta que, fruto de la revisión de esta documentación queda patente que el poder de dirección estaba en manos de la matriz *Facebook Inc* que era el responsable del tratamiento[520].

Asimismo, aunque el papel de la sociedad belga es meramente consultivo, en virtud del asunto *Google Spain SL*, la autoridad entiende aplicable la legislación belga, al considerar a *sprl Facebook Belgium* como un establecimiento del responsable ubicado en territorio belga[521]. Las actividades de este establecimiento se considera que están indisociablemente unidas a las actividades del responsable, independientemente de que este establecimiento ejerza o no las actividades concretas del tratamiento.

La aplicación del criterio también tendría sentido en el caso de que una ley nacional estime que el elemento subjetivo del responsable del tratamiento no lo compone un establecimiento que, sin embargo, sí puede desencadenar la aplicación del criterio de aplicación de la ley. Por ejemplo, si estamos ante una sucursal que no tiene personalidad jurídica y la ley nacional no permite que sea responsable del tratamiento una entidad sin personalidad jurídica. Entonces será útil que se considere a este establecimiento, dependiente de una empresa matriz, como un establecimiento que podría desencadenar la aplicación de la ley.

También podemos pensar en otro tipo de establecimientos que podrían no reunir los requisitos para ser responsable del tratamiento. En estos casos es cuando tendrá sentido aplicar el criterio de la Directiva 95/46/CE. Para aplicar este criterio, como he indicado anteriormente debería utilizarse la misma técnica que para identificar al responsable del tratamiento. De esta forma, deberá contemplarse si ese establecimiento es el que determina los fines y los medios del tratamiento o es otro establecimiento dentro de la organización del responsable el que lo hace[522].

---

[520] *Ibídem*, págs. 6 a 8.

[521] Curiosamente, la sociedad belga se había creado para ejercer como *lobby* en el proceso de reforma de la Directiva 95/46/CE. *Recommandation nº 04/2015 du 13 mai 2015, Comission de la protection de la vie privée*, págs. 8 a 15.

[522] También parece optar por esta solución J. APARICIO SALOM, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, 4ª ed, *op. cit.*, págs. 41 a 48.

2. APLICACIÓN DE LA LEY DE UN ESTADO MIEMBRO EN VIRTUD DEL DERECHO INTERNACIONAL PÚBLICO: EL SEGUNDO CRITERIO

El segundo supuesto que establece el artículo 4.1.b) Directiva 95/46/CE es el relativo al responsable del tratamiento establecido en un lugar en que se aplica la legislación del Estado miembro en virtud del derecho internacional público. En el mismo confluyen dos requisitos. El primero es que el responsable del tratamiento no esté establecido en el territorio del Estado miembro y, por tanto, que no se desencadene la aplicación del artículo 4.1.a) Directiva 95/46/CE. El segundo requisito es que criterios de derecho internacional público determinen la aplicación del derecho nacional de protección de datos fuera de las fronteras nacionales. Esto ocurre en el caso de las embajadas, consulados, buques, aeronaves, en los que el derecho internacional público o acuerdos internacionales puedan determinar la legislación aplicable[523].

3. EL RESPONSABLE DEL TRATAMIENTO NO ESTÁ ESTABLECIDO EN LA UNIÓN EUROPEA/ESPACIO ECONÓMICO EUROPEO: EL TERCER CRITERIO

El tercer criterio que establece la Directiva 95/46/CE es el que pretende extender la protección hacia aquellos responsables que se ubiquen fuera del EEE, como indica en su preámbulo:

> "Considerando que el hecho de que el responsable del tratamiento de datos esté establecido en un país tercero no debe obstaculizar la protección de las personas contemplada en la presente Directiva; que en estos casos el tratamiento de datos debe regirse por la legislación del Estado miembro en el que se ubiquen los medios utilizados y deben adoptarse garantías para que se respeten en la práctica los derechos y obligaciones contempladas en la presente Directiva" (Considerando 20 Directiva 95/46/CE).

De esta forma se aplicará la ley nacional cuando:

> "el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea" (art. 4.1.c) Directiva 95/46/CE).

[523] Dictamen 8/2010 sobre el derecho aplicable, *op. cit.*, pág. 20. Este criterio se ha recogido en la LOPD, en su artículo 2.1.b) y se reproduce en el artículo 3.1.b) RLOPD sin contener ninguna modificación relevante. Ambos artículos disponen que se aplicará la legislación española cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de las normas de derecho internacional público.

Lo primero que señala el GA29 respecto a este criterio es que no puede aplicarse el mismo si fuera posible aplicar el primer criterio[524]. Es decir, sólo si el responsable carece de un establecimiento relevante para activar el primer criterio podrá aplicarse este tercer criterio, siempre que se cumplan los requisitos que el mismo dispone[525] y que se estuviera ante el mismo tratamiento de datos personales[526].

Respecto a la transposición del criterio en las leyes nacionales, si no se tienen en cuenta las diferencias que después se mencionarán referentes a la cuestión del territorio al que debe referirse la utilización de medios con fines de tránsito, alrededor de la mitad de las leyes estarían en sintonía con la Directiva 95/46/CE[527].

No obstante, hay que señalar las divergencias que se han producido en las otras leyes nacionales. Así, además de las que mencionaré durante los próximos apartados, hay que resaltar que algunas leyes han previsto lo que significa no estar establecido en el territorio de la UE y otras incluso se refieren a responsables que podrían estar establecidos en la UE, claramente en contra de lo indicado en la Directiva 95/46/CE[528].

[524] *Ibídem*, pág. 22.

[525] De esta forma, el GA29 indica que si el responsable del tratamiento tuviera establecimientos en la UE pero sus actividades no estuvieran relacionadas con el tratamiento de datos personales, no podría aplicarse el artículo 4.1.a) Directiva 95/46/CE. *Ibídem*, pág. 22.

[526] En este sentido, se podría activar la aplicación de ambas disposiciones si el responsable del tratamiento establecido fuera de la UE recurre a medios en la UE y, por otro lado tiene un establecimiento en la UE, en el marco del que trata datos personales para otras actividades diferentes. *Ibídem*.

[527] En concreto y, como se indica, sin perjuicio de lo referido con relación al territorio al que se circunscribe la excepción referida a la utilización de los medios con fines de tránsito, se puede decir, respecto al resto, que respetan la redacción de este tercer criterio, tal como se describe en la Directiva 95/46/CE, las siguientes leyes: la Ley búlgara (art. 1.4.3), la Ley chipriota (art. 3.3.b), la Ley eslovena (art. 5.2), Ley finlandesa (art. 4.2), la Ley francesa (art. 5.I.2º), la Ley griega (art. 3.3.b), la Ley Países Bajos (art. 4.2), la Ley italiana (Sección 5.2), Ley irlandesa (3B.a.ii), Ley letona (art. 3.1.3), Ley lituana (art. 1.3.3), Ley luxemburguesa (art. 3.2.b), Ley maltesa (art. 4.2), Ley portuguesa (art. 4.3.c), Ley inglesa (art. 5.1.b), Ley de Liechtenstein (art. 2.2.c) y la Ley noruega (art. 4).

[528] Las Leyes belga y eslovaca han especificado que se considera que es no estar establecido en el territorio de la Unión Europea, lo que iría más allá de lo contemplado por este tercer criterio en la Directiva 95/46/CE. Así, la Ley belga precisa como única diferencia en lo relativo a este criterio que "se aplicará la ley al responsable del tratamiento no establecido de forma permanente en el territorio de la Comunidad Europea" (art. 3bis.2 Ley belga, el subrayado es de la autora). Por su parte, la Ley eslovaca concreta los tipos de establecimiento que no debe tener el responsable en el territorio de un Estado miembro (oficina registrada, unidad organizativa, establecimiento de negocio o residencia permanente) para que pueda aplicarse el mismo (sección 2.2.b Ley eslovaca, el subrayado es de la autora). Las Leyes rumana y chipriota se aplicarán al tratamiento que se lleve a cabo en el marco de las actividades de responsables no establecidos en estos países que utilicen medios en sus territorios, a no ser que se utilicen con fines de tránsito a través de estos territorios. Por tanto, estas leyes se refieren a responsables establecidos fuera de Rumanía y de Chipre, por lo que también se incluirán responsables que estén ubicados en la Unión Europea, lo que iría en contra de lo establecido por la Directiva 95/46/CE (art. 2.2.c Ley rumana y art. 3.3.b Ley chipriota)

También hay leyes que amplían o restringen el criterio o que lo adaptan a sus especiales características[529].

3.1. El recurso a medios

En lo que respecta al recurso a medios, automatizados o no, situados en el territorio del Estado miembro, el GA29 señala que este recurso presupone dos elementos: algún tipo de actividad del responsable del tratamiento y la clara intención del mismo de tratar datos personales[530]. Por tanto, en principio lo que el GA29 indica es que se debe evitar la aplicación de la ley, en caso de un tratamiento de datos "accidental" por parte del responsable del tratamiento.

En la versión inglesa se utiliza la palabra "*equipment*", en lugar de "*means*", que sería la que equivaldría al término "medios" que se utiliza en las otras versiones. En este sentido, como indica el GA29, la utilización del término medios estaría en coherencia con la definición del responsable que alude a su capacidad de determinar los fines y los medios del tratamiento de datos personales. Sin embargo, el mismo GA29 especifica que no es preciso que el responsable del tratamiento tenga la propiedad o ejerza el pleno control de dichos medios para que el tratamiento se someta al ámbito de aplicación de la directiva.

En todo caso, estimo que sí debería tener la capacidad de determinar los medios y todo lo que se refiere a los mismos, ya que debe estar en consonancia con la definición de

[529] La Ley danesa amplía el alcance del criterio porque lo aplica respecto a responsables establecidos en lo que se define como un país tercero, que es el que no es miembro de la UE o que no tiene ningún acuerdo con la UE que contenga reglas equiparables a las de la Directiva 95/46/CE (art. 4.3.1 Ley danesa). Asimismo, otra diferencia de la Ley danesa es que establece que se aplicará a responsables ubicados en un país tercero si la recogida de datos realizada en Dinamarca se lleva a cabo con el propósito de tratarlos en el país tercero (art. 4.3.2 Ley danesa). Por otro lado, la Ley polaca restringe el alcance de este criterio sólo al sector privado (art. 3 Ley polaca). Por último, la Ley alemana en lugar de referirse al tratamiento que realiza el responsable utilizando medios que se ubiquen en el territorio de Alemania, indica que "recoja, trate o use datos personales" (sección 1.5 Ley alemana). Esta referencia es resultado de la peculiar regulación de la ley alemana que en vez de tratamiento, separa las operaciones a que se someten los datos personales en tres tipos (recogida, tratamiento y uso).

[530] Dictamen 8/2010 sobre el derecho aplicable, *op. cit.*, pág. 23 y Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE, *op. cit.*, pág. 10. No obstante, hay que señalar que si bien la versión en español de la Directiva 95/46/CE alude a "recurrir a medios", lo que da una idea de esta voluntad consciente del responsable de tratar datos, en la versión inglesa de la directiva se alude a "*makes use*", que no da esa idea tan clara de consciencia en esa utilización, sino que simplemente se utilizan.

responsable. En este sentido, el GA29 apunta que el control sobre los medios será suficiente cuando el responsable, al determinar la forma en que los medios funcionan, tome las decisiones adecuadas respecto a la naturaleza de los datos y su tratamiento, lo que equipara a determinar qué datos se recogen, se almacenan, se transfieren, se modifican, de qué forma y con qué objetivo[531].

El término medios se interpreta de forma amplia, por lo que incluye intermediarios humanos o técnicos[532]. Asimismo, el GA29 entendió como medios, el recurso a los ordenadores de los usuarios que acceden a un sitio web, cuando el responsable del tratamiento que está detrás de este sitio web utiliza cookies o archivos *Javascript*[533]. Esta interpretación fue bastante polémica ya que la mayoría de sitios web utilizan este tipo de archivos, de forma que se ampliaba de forma extraordinaria el ámbito de aplicación de la Directiva 95/46/CE[534].

Además, tal como también confirma el GA29, se podrá entender como una utilización de medios, el recurso por parte del responsable del tratamiento establecido fuera del EEE a encargados de tratamiento[535]. De hecho, hay algunas leyes nacionales que, al transponer este criterio, han previsto que la utilización de medios en realidad lo que quiere decir es la utilización de encargados del tratamiento ubicados en el Estado miembro[536].

---

[531] Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE, 5035/01/ES/Final WP 56, 30.5.2002, Grupo de trabajo Artículo 29 sobre la protección de datos, pág. 10.

[532] Como cita de otra divergencia en las leyes nacionales, cabe mencionar la Ley polaca que se refiere a medios técnicos, lo que parece apuntar únicamente a medios automatizados (art. 3 Ley polaca). La ley islandesa establece la utilización de medios y facilidades situados en Islandia (art.6 Ley islandesa).

[533] Dictamen 8/2010 sobre el derecho aplicable, *op. cit.*, pág. 24 y Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE, *op. cit.*, págs. 10 a 13.

[534] Por eso, en el Dictamen 8/2010 el GA29 admite que la interpretación de esta disposición favorece una aplicación muy amplia de la Directiva 95/46/CE que, en algunos casos podría aplicarse a supuestos en los que la conexión con la UE fuera muy limitada y cita como ejemplo el caso en que un responsable de fuera de la UE tratara datos de personas no residentes en la UE pero que, al utilizar medios que estuvieran en territorio de la UE activara la aplicación de la directiva. Dictamen 8/2010 sobre el derecho aplicable, *op. cit.*, pág. 24. En este sentido, la AEPD entendió aplicable este criterio plasmado en el artículo 2.1.c) LOPD en un procedimiento sancionador seguido contra *Google* por el uso de las cookies que realizaba la empresa estadounidense. Resolución R/02892/2013 de 18 de diciembre de 2013, en Procedimiento nº PS/00345/2013.

[535] Dictamen 8/2010 sobre el derecho aplicable, *op. cit.*, págs. 23 a 24.

[536] En este sentido, hay que destacar que la Ley húngara, en lugar de referirse al recurso de medios en territorio de Hungría, ha entendido que medios sólo puede referirse a un supuesto de contratación de un encargado del tratamiento que tenga su sede, ubicación, filial o dirección o lugar de residencia en el

3.2. La excepción relativa a la utilización de medios con fines de tránsito

Por lo que se refiere a la excepción que contempla el artículo 4.1.c) Directiva 95/46/CE relativa al supuesto en el que los medios se utilicen con fines de tránsito por el territorio de la UE, hay que entender que se alude a aquellos medios que sirven para que se puedan efectuar las comunicaciones (como las redes de telecomunicaciones o servicios postales). Al ser una excepción debe interpretarse estrictamente de forma que los medios sirvan exclusivamente para una transmisión "punto a punto" sin incluir ningún tipo de manipulación de los datos que circulan[537].

La mayoría de las leyes de los Estados miembros han cambiado la referencia que se realiza en la Directiva 95/46/CE al territorio de la UE con la finalidad de delimitar geográficamente el área donde se permite utilizar los medios con fines de tránsito. Estas leyes, en su mayoría, han modificado esta referencia por la relativa al país en cuestión por entender que se trataba de una referencia que se debía modificar para amoldarla al Estado.

Sin embargo, el sentido de aludir al territorio de la UE es facilitar que puedan transmitirse informaciones a través de las redes que atraviesan el territorio del EEE[538], sin que ello requiera la aplicación de la normativa. Por ello, la alusión a la UE tiene el objetivo de explicar la finalidad de la excepción, el libre tránsito de la información a través del territorio del EEE. Los Estados miembros que han cambiado esta disposición

territorio de Hungría para llevar a cabo el tratamiento de datos (Sección 2.3 Ley húngara). La Ley checa respecto a este criterio no se refiere a medios, de forma que entiende que se aplicará la ley si el responsable que se encuentra fuera de la UE realiza un tratamiento de datos en el territorio checo, excepto si es sólo para la transferencia de datos por el territorio de la UE, por lo que apunta claramente a la presencia de un encargado del tratamiento. A continuación la ley indica que el responsable deberá autorizar al encargado del tratamiento en el territorio de la República Checa lo que implica seguir la regulación para esta delegación en el artículo 6 Ley checa, que exige establecerlo mediante un contrato con éste, a no ser que sea una ley la que lo autorice. Por tanto, en este caso, se ha sustituido la designación del representante por la designación de un encargado del tratamiento. La Ley checa transforma la alusión a medios por una alusión a un encargado del tratamiento (art. 3.5.b) Ley checa). Por último, mencionar la Ley austríaca que, simplemente indica, que este criterio se aplicará a los usos de datos personales que se lleven a cabo en Austria (§ 3.1 Ley austríaca).

[537] Como apunta el GA29 este tipo de servicios es cada vez más escaso ya que se suelen incorporar servicios de valor añadido. Dictamen 8/2010 sobre el derecho aplicable, *op. cit.*, pág. 26.

[538] Hay que recordar que al indicar el territorio de la Comunidad en la Directiva 95/46/CE equivale a indicar el territorio de los Estados miembros de la UE y los que conforman el Espacio Económico Europeo (Islandia, Liechtenstein y Noruega).

han entendido que al tener competencia sobre su territorio debían incluir en la excepción su territorio únicamente y, por tanto, el tránsito sólo se efectuaría en su territorio.

Las leyes que han seguido el sentido de la disposición y, por tanto, han contemplado el territorio de forma global en coherencia con la Directiva 95/46/CE son únicamente las Leyes de Dinamarca, República Checa, Portugal, Francia, Luxemburgo, República de Eslovaquia y Liechtenstein[539]. La ley española no hace referencia a ningún territorio sino que se limita a indicar que se excepcionará la aplicación del criterio si los medios se utilizan "únicamente con fines de tránsito" (arts. 2.1.c) LOPD y 3.1.c) RLOPD).

Asimismo, también hay que resaltar las leyes de Austria y Estonia que han establecido que, este supuesto en el que los datos son tratados con fines de tránsito en el territorio de estos países no se aplicará la ley de protección de datos[540]. Así, este supuesto, en vez de constituir una excepción a uno de los criterios de aplicación de la norma, se convierte en una exclusión directa de la aplicación general de la ley.

3.3. La designación de un representante

Respecto al tercer criterio el responsable del tratamiento, establecido fuera del EEE, deberá designar un representante establecido en el territorio del Estado miembro donde se ubiquen los medios utilizados por este responsable (art. 4.2 Directiva 95/46/CE).

No obstante, se precisa que la designación del representante no impide que puedan emprenderse acciones contra el propio responsable del tratamiento. Cabe plantearse, por tanto, cual es la responsabilidad concreta del representante que ni se aborda en la Directiva 95/46/CE ni encuentra una respuesta uniforme en las legislaciones nacionales.

[539] Sin embargo, incluso en este reducido grupo de leyes hay divergencias en la forma de aludir al territorio: las Leyes danesa, checa y portuguesa se refieren al territorio de la UE, la Ley francesa se refiere a Francia o cualquier Estado miembro, al igual que la Ley luxemburguesa que indica Luxemburgo o cualquier Estado miembro. La Ley eslovaca se refiere al territorio de los Estados miembros (Sección 2.2.b Ley eslovaca). La Ley de Liechtenstein, como no podía ser de otra manera, se refiere al EEE, ya que este Estado aplica la Directiva 95/46/CE al ser parte de este acuerdo.

[540] § 3.3 Ley austríaca y artículo 2.1.2 Ley estonia.

Al examinar la transposición de esta previsión de la Directiva 95/46/CE a las leyes nacionales, se observan de nuevo divergencias en la regulación. De esta forma, se obtienen un gran número de variaciones. Desde las leyes que se limitan a incluir una obligación de designar al representante sin más, como sucede en la ley española[541], hasta las leyes que transponen de forma similar esta disposición[542], alguna ley que no contempla siquiera la obligación de nombrarlo[543] y las leyes que han estimado ir más allá de lo establecido en la directiva.

Estas leyes que han ido más allá de lo que indica la Directiva 95/46/CE especifican, o bien que el representante se asimilará al responsable, de forma que sustituiría al mismo en el cumplimiento de sus obligaciones establecidas en la ley pertinente[544], o que el representante deberá cumplir con las disposiciones previstas en la ley[545]. Asimismo, algunas leyes nacionales especifican un poco más el tipo de establecimiento que debe tener el representante o su forma jurídica[546]. También en algunas normas se establece la necesidad de que el responsable comunique a la autoridad de control la designación del representante[547]. Varias leyes dejan claro que el responsable

[541] Incluyen esta obligación de designar al representante sin más: el artículo 3.1.c LOPD, la Ley alemana simplemente indica que se debe designar responsable (sección 1.5 Ley alemana), el artículo 7.6) Ley estonia, el artículo 4.2 Ley finlandesa, el artículo 2.3 Ley húngara, el artículo 4.2 Ley maltesa, el artículo 31a Ley polaca, el artículo 5.2 Ley inglesa y el artículo 2.2.c) Ley de Liechtenstein.

[542] Las Leyes belga e irlandesa establecen que el responsable del tratamiento debe designar un representante establecido en el territorio belga, sin perjuicio de acciones que puedan interponerse contra el responsable mismo (art. 3bis.2 Ley belga y art. 3B.c Ley irlandesa). En la Ley búlgara se reproduce la previsión de la directiva aunque resulta confuso que en referencia a la designación del representante por parte del responsable especifica que: "*this, however, shall relieve it from responsability*" (art. 1.4.3 Ley búlgara).

[543] La Ley checa no establece la necesidad de designar un representante, ya que lo que hace es entender que cuando el responsable establecido fuera de la UE realiza un tratamiento de datos en el territorio checo es porque recurre a un encargado del tratamiento (art. 3.5 Ley checa).

[544] Así, la Ley austríaca indica que cuando el responsable esté establecido fuera de la UE debe designar representante que podrá considerarse responsable, sin perjuicio de las acciones contra el propio responsable (§ 6.3 Ley austríaca). De forma similar se contempla esta previsión en el artículo 3.3.b Ley griega, artículo 5.II Ley francesa, artículo 4.3 Ley Países Bajos, artículo 3.2 Ley luxemburguesa, artículo 4.5 Ley portuguesa, artículo 3.3.b Ley chipriota.

[545] Así establecen que las disposiciones de la ley de protección de datos también se le aplicarán al representante: la sección 7 Ley eslovaca, la Sección 5.2 Ley italiana, el artículo 3.2 Ley letona, el artículo 1.3.3 Ley lituana, el artículo 2.3 Ley rumana, la sección 4 Ley sueca, el artículo 6 Ley islandesa y el artículo 4 Ley noruega.

[546] La Ley eslovaca precisa que el representante debe contar con una oficina registrada, un lugar de negocio o residencia permanente en el territorio de Eslovaquia de forma previa al inicio del tratamiento de datos personales (sección 4.2.c) y sección 7 Ley eslovaca). La Ley eslovena especifica que el representante puede ser una persona física o jurídica que resida o esté registrado en la República de Eslovenia (art. 5.3 Ley eslovena). La Ley lituana indica que el responsable debe tener un representante que será una filial o una oficina de representación en Lituania (art. 1.3.3 Ley lituana).

[547] El artículo 3.3.b Ley chipriota, el artículo 4.3.1. Ley danesa, el artículo 3.3.b) Ley griega y el artículo 3.2 Ley luxemburguesa obligan a que la designación sea por escrito y se comunique a la autoridad de control.

debe designar al representante aunque el responsable ostentara algún tipo de inmunidad[548].

4. LEGISLACIÓN APLICABLE AL ENCARGADO DEL TRATAMIENTO

Tal como ya se ha indicado y en el marco del tercer criterio sobre la ley aplicable, se podrá entender, como una utilización de medios, el recurso, por parte del responsable del tratamiento establecido fuera del EEE, a encargados de tratamiento.

No obstante, también hay que tener en cuenta que, en un supuesto en el que el responsable esté establecido fuera del EEE y tuviera algún establecimiento en el EEE, que implicara la aplicación del primer criterio del artículo 4.1.a) Directiva 95/46/CE, si este establecimiento recurriera a algún encargado del tratamiento, debería aplicarse la ley del Estado miembro donde esté ubicado el establecimiento. La razón es que como se ha dicho se otorga prevalencia al primer criterio sobre el tercero. Así lo afirma también la Directiva 95/46/CE, en su preámbulo, cuando indica que el tratamiento de datos efectuados por cualquier persona que actúe bajo la autoridad del responsable del tratamiento establecido en un Estado miembro, se someterá a la aplicación de la legislación de tal Estado (Considerando 18 Directiva 95/46/CE)[549].

En lo que respecta a los encargados del tratamiento hay que mencionar la regulación específica de las medidas de seguridad que deben adoptar. El contrato o acto jurídico que debe vincular al encargado del tratamiento con el responsable del tratamiento debe disponer, además de que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento, que las obligaciones relativas al cumplimiento de las medidas de seguridad, "tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste" (art. 17.3

El artículo 5.II Ley francesa y el artículo 4.5 Ley portuguesa obligan a notificarlo a la autoridad de control, sin precisar si deben hacer la designación por escrito.

[548] El artículo 3.3.b) Ley griega especifica que la obligación de designar representante se aplicará aunque el responsable contara con algún tipo de inmunidad. La Ley portuguesa amplía la obligación de designación de representante para los casos en que el responsable estuviera cubierto por un estatus de extraterritorialidad, inmunidad o cualquier otro estatuto que le exima de ser imputado en procedimientos penales (art. 4.6 Ley portuguesa).

[549] D. SANCHO VILLA, "Ámbito de aplicación territorial", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, *op. cit.*, pág. 102.

Directiva 95/46/CE)[550]. Por tanto, según esta disposición, las medidas de seguridad que debe aplicar el encargado serán las definidas por el Estado miembro donde éste se ubique. Este aspecto ha tenido reflejo en algunas de las leyes nacionales, aunque de manera diversa[551].

La legislación española incluye también esta previsión, al establecer el primer criterio de determinación de la ley aplicable (art. 3.1.a) RLOPD que transpone el artículo 4.1.a Directiva 95/46/CE). De esta forma, el RLOPD indica que, cuando no se pueda aplicar este primer criterio pero exista un encargado del tratamiento ubicado en España, se le aplicará la regulación relativa a las medidas de seguridad que deben aplicarse para proteger los datos tratados (contenidas en el Título VIII RLOPD). Por tanto, si no se puede considerar que existe un establecimiento del responsable del tratamiento en el marco de cuyas actividades se realice el tratamiento pero sí hay un encargado del tratamiento, se aplicará esa parte de la normativa relativa a las medidas de seguridad.

[550] El GA29 arguye que la razón de esta previsión es garantizar que se apliquen los mismos requisitos sobre las medidas de seguridad en el marco de un mismo Estado miembro. Resalta el grupo que la regulación en materia de medidas de seguridad se diferencia en las diversas leyes nacionales que aplican la Directiva 95/46/CE, de forma que algunas se han limitado a dejar una regulación general, como en la directiva, mientras que en otras se establece una regulación detallada (como en España). Esto podría implicar que el responsable del tratamiento contrate un encargado del tratamiento en un Estado miembro que tenga unas obligaciones menos estrictas en materia de seguridad que las que pudiera tener el responsable del tratamiento si aplicara la ley del Estado miembro donde estuviera establecido. Por tanto, indica el grupo la necesidad de buscar una mayor armonización en la regulación de estas medidas de seguridad. Dictamen 8/2010 sobre el derecho aplicable, *op. cit.*, pág. 29.

[551] En este sentido, la Ley griega cuando establece el ámbito de aplicación territorial indica expresamente que será aplicable a los tratamientos realizados por los encargados del tratamiento que se ubiquen en el territorio griego o en un lugar sometido a la Ley griega en virtud de derecho internacional público (art. 3.3.a Ley griega). La Ley danesa especifica que si el encargado del tratamiento se halla establecido en otro Estado miembro, el contrato entre el responsable y el encargado debe estipular que las medidas de seguridad que haya dispuesto la legislación de ese Estado también debe cumplirlas el encargado (art. 42.2 Ley danesa). La Ley Países Bajos indica que, cuando el encargado se halle establecido en otro país de la UE, el responsable deberá asegurarse de que el encargado cumpla con las leyes de ese otro país (art. 14.4 Ley Países Bajos). La Ley islandesa dispone que si el encargado estuviera establecido en otro Estado en el EEE diferente de aquel donde esté el responsable deberá estipularse en el contrato que las leyes y regulaciones del Estado donde el encargado está establecido serán las aplicables respecto a las medidas de seguridad del tratamiento (art. 13 Ley islandesa).

CAPÍTULO V

EL ESTATUTO DEL RESPONSABLE EN LA DIRECTIVA 95/46/CE Y EN LAS LEGISLACIONES NACIONALES EUROPEAS

La Directiva 95/46/CE puede contemplarse desde la perspectiva del sujeto protegido o también desde la del sujeto obligado. En el primer caso, en un análisis de la regulación se atendería fundamentalmente a los derechos que se extraen de la directiva. En el segundo caso, este enfoque, que es el que seguiremos en las siguientes páginas, nos hará extraer las obligaciones que derivan de la norma para los responsables que tratan datos personales y algunas facultades o derechos que vendrán implícitos en el marco de estas obligaciones. De este estudio se deducirá el estatuto del responsable[552].

Para ofrecer una visión europea de este catálogo de obligaciones y derechos del responsable, es necesario partir de la norma base que es la Directiva 95/46/CE. Sin embargo, al tratarse la Directiva 95/46/CE de una norma instrumental, que obliga a los Estados miembros a adoptar una normativa que es la realmente aplicable, apuntaré algunas características de estas leyes y especialmente de las divergencias observadas respecto a la Directiva 95/46/CE[553].

1. LA FALTA DE ARMONIZACIÓN EN LA REGULACIÓN EUROPEA DEL ESTATUTO

El resultado extraído del análisis del marco europeo de regulación del estatuto del responsable, es que hay una falta de armonización en las legislaciones nacionales, lo que denota que no se ha conseguido el objetivo que pretendía el legislador comunitario con la

[552] De hecho, durante el proceso de negociación en la elaboración de la Directiva 95/46/CE se propuso que el apartado 2 del artículo 6, en el que se asigna expresamente el cumplimiento de los principios de calidad al responsable del tratamiento, formara parte de un precepto que regulara el estatuto del responsable del tratamiento. Este precepto podría haber recogido las demás funciones atribuidas al responsable en los artículos 17, 8.2.b, 10, 11, 12, 14, 16, 17, 18, 19 y 23, según afirma M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, pág. 107.

[553] No se incluyen en el análisis las normativas de desarrollo de las leyes principales relativas a la materia de la protección de datos ni tampoco las normas sectoriales que pudieran contener regulación en esta materia o que le afecte de algún modo. El estudio del estatuto del responsable en el derecho español se abordará en el Capítulo VI, por lo que sólo se apuntarán algunas de las divergencias que después se contemplarán con más profundidad.

Directiva 95/46/CE[554]. No obstante, hay que decir que, no todas las diferencias existentes en la legislación nacional son fruto de transposiciones incorrectas de la Directiva 95/46/CE. Algunas de estas divergencias son fruto del margen de maniobra que permite la Directiva 95/46/CE[555].

Aunque se entienda que la Directiva 95/46/CE realiza una armonización completa, se incluyen, en la misma, algunas normas que permiten cierta flexibilidad a los Estados miembros[556]. La más clara es el artículo 13 Directiva 95/46/CE que permite a los Estados miembros limitar el alcance de algunos de los derechos que otorga a los interesados y de las obligaciones de los responsables del tratamiento. El TJUE ha confirmado que esta disposición confiere una facultad y no una obligación para los Estados[557]. Esta facultad viene condicionada por la consecución de los objetivos establecidos en el precepto[558] y por el criterio de necesidad que debe regir a la hora de que los Estados adopten estas medidas limitadoras[559].

En concreto esta disposición posibilita la limitación de las obligaciones y los derechos previstos en los siguientes preceptos de la Directiva 95/46/CE: el artículo 6.1 (principios de calidad), artículo 10 (información del interesado cuando los datos se recaban del propio interesado), artículo 11.1 (información del interesado cuando los datos no son recabados del propio interesado, artículo 12 (derecho de acceso) y artículo 21 (publicidad de los tratamientos).

---

[554] Así concluye la Comisión Europea del estudio realizado sobre la regulación en esta materia, que no hace sino confirmar los resultados que se obtuvieron en los exámenes de la normativa de transposición de los años 2003 y 2007. *Commission Staff Working Paper, Impact assessment accompanying the document Regulation of the European Parliament […], op. cit.*, pág. 47.

[555] O. TENE, "Reforming data protection in Europe and beyond", A. RALLO LOMBARTE, R. GARCÍA MAHAMUT (Ed.), VVAA, *Hacia un nuevo derecho europeo de protección de datos. Towards a new European data protection regime, op. cit.*, pág. 153.

[556] Sentencia del TJUE de 6 de noviembre de 2003 *Bodil Lindqvist*, C-101/01, EU:C:2003:596, apdos. 83, 95-96.

[557] Sentencia del TJUE de 7 de noviembre de 2013, *IPI*, C-473/12, EU:C:2013:715.

[558] Los objetivos que permiten que el Estado miembro pueda adoptar estas limitaciones son: salvaguardar la seguridad del Estado; la defensa; la seguridad pública; la prevención, la investigación, la detección y la represión de infracciones penales o de infracciones de deontología de las profesiones reglamentadas; el interés económico y financiero; el control, inspección u otra función reglamentaria relacionada con el ejercicio de la autoridad pública en relación con los puntos anteriores relativos a la seguridad pública, las infracciones penales o el interés económico y financiero; la protección del interesado o de los derechos y libertades de otras personas (art. 13.1 Directiva 95/46/CE). Asimismo, los Estados miembros también pueden limitar el derecho de acceso (art. 12 Directiva 95/46/CE) por disposición legal cuando los datos se vayan a tratar con fines de investigación científica o para la elaboración de estadísticas (art. 13.2 Directiva 95/46/CE).

[559] Sentencia del TJUE de 7 de noviembre de 2013, *IPI*, C-473/12, EU:C:2013:715, apdo. 32.

La existencia de estas divergencias en las leyes nacionales dificulta especialmente el cumplimiento por parte de los responsables que se encuentran ubicados en varios Estados miembros. Asimismo, en una sociedad tecnológica como la actual, esto origina prácticas de *forum shopping*, mediante las que las empresas buscan el Estado que tenga la legislación más laxa para ubicar allí sus establecimientos. Si bien no hay que disminuir en ningún caso la protección de los derechos fundamentales, resulta contraproducente incrementar la carga que debe soportar el sujeto obligado, ya que, finalmente, se consigue el efecto contrario al perseguido[560].

2. LA ASIGNACIÓN DE OBLIGACIONES

Del examen de la Directiva 95/46/CE se extrae un catálogo de obligaciones para el responsable que, en algunos casos se asignan de forma expresa y, en otros, se infieren de la norma. En aras de obtener una visión pragmática del estatuto, se incluirán todas ellas y se presentarán, para su análisis, de acuerdo con el circuito lógico que sigue un tratamiento de datos personales.

Las principales fases que sigue todo tratamiento de datos, y que entiendo son importantes desde el punto de vista de las obligaciones, son: la entrada de los datos personales en la organización responsable, la circulación de estos datos en el seno de la organización y la de salida de datos hacia el exterior de la organización, ya sea hacia encargados del tratamiento, o hacia terceros a los que se comunican los datos[561].

Algunas obligaciones claramente se refieren a las fases de entrada o salida, mientras que otras tienen un carácter transversal, de forma que pueden producirse en cualquiera de las fases del ciclo y, especialmente en la de circulación, mientras los datos se tratan dentro de la organización.

---

[560] El TJUE mencionaba la necesidad de que las obligaciones del responsable fueran proporcionadas. Sentencia del TJUE de 7 de mayo de 2009, *College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer*, C-553/07, EU:C:2009:293, apdo. 62.

[561] Otros autores también han adoptado enfoques similares y han analizado la regulación, en virtud de las fases del proceso informático, como RIASCOS GÓMEZ, al que se remite QUESADA. L.O. RIASCOS GÓMEZ, *El derecho a la intimidad, la visión iusinformática y el delito de los datos personales*, Tesis doctoral, Universitat de Lleida, Lleida, 1999, págs. 196 a 213, 376 a 431. A. QUESADA RODRÍGUEZ, *Protección de datos y telecomunicaciones convergentes, Premio protección de datos personales de investigación 2014*, *op. cit.*, págs. 168 a 176.

En la fase de entrada de datos, el responsable deberá cumplir las obligaciones referidas: a la legitimación del tratamiento de datos personales (art. 7 Directiva 95/46/CE) y, en especial, del tratamiento de categorías especiales de datos (arts. 8 y 9 Directiva 95/46/CE), así como a la información al interesado (arts. 10 y 11 Directiva 95/46/CE)[562] y a la notificación del tratamiento de datos a la autoridad de control (arts. 18 a 21 Directiva 95/46/CE).

Son obligaciones transversales que deberán cumplirse durante todo el ciclo del tratamiento: los principios de calidad (art. 6 Directiva 95/46/CE), la atención de los derechos que puedan ejercer los interesados de acceso, de oposición y de no verse sometidos a decisiones individuales automatizadas (arts. 12, 14 y 15 Directiva 95/36/CE), el deber de confidencialidad y de seguridad (arts. 16 y 17 Directiva 95/46/CE) y el sometimiento a los poderes de investigación y a los poderes de intervención de la autoridad de control (art. 28.3 Directiva 95/46/CE).

Las obligaciones que afectarían a la fase de salida serían las relativas a la regulación del encargo del tratamiento (art. 17.2 y 3 Directiva 95/46/CE) y a las transferencias de datos a países terceros (art. 25 Directiva 95/46/CE).

Las listas indicadas de obligaciones deberían completarse, en el ámbito de los ordenamientos de los Estados miembros, con otras normativas que puedan ser aplicables, ya sea porque remite la propia ley de protección de datos que transpone la Directiva 95/46/CE o porque se puedan encontrar, en estas leyes, disposiciones específicas sobre el tratamiento de datos.

No hay que olvidar que la protección de datos es una materia transversal[563]. Los responsables del tratamiento están habilitados para tratar datos, como se verá, con el fin de cumplir con sus obligaciones legales, para ejecutar contratos o para perseguir el interés

[562] En referencia a la obligación de informar cuando los datos no provienen directamente del afectado (art. 11 Directiva 95/46/CE) hay que tener en cuenta que se establece un límite temporal para cumplir con esta obligación que se refiere al momento de comunicar los datos a un tercero. Por tanto, esta obligación concreta se debería cumplir justo antes de la salida de datos.

[563] Ejemplos de ello se encuentran en la misma Directiva 95/46/CE que recoge en diversas de sus disposiciones regulaciones dirigidas a actividades o sectores en concreto (las disposiciones que regulan las categorías especiales de tratamientos, Sección III, Capítulo II Directiva 95/46/CE).

público. Estas finalidades se enmarcan en una regulación legal que cuanto más ligada esté al tratamiento de datos, más probable es que pueda incluir preceptos que regulen el mismo[564]. Esta adición de normativas, que se deben tener en cuenta, puede ser un factor que incentive la aparición de discordancias y dificultades para el responsable, a la hora de cumplir con sus obligaciones, por ejemplo, si se produjera una contradicción entre ambas normas, la sectorial y la de protección de datos.

3. OBLIGACIONES EN LA FASE DE ENTRADA DE LOS DATOS PERSONALES

3.1. La legitimación para tratar datos

La importancia de la legitimación se refleja en que la Carta UE, en su formulación del derecho a la protección de datos, establece que los datos se tratarán "sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley" (art. 8.2 Carta UE).

Los artículos 6 y 7 Directiva 95/46/CE, en su título, hacen referencia a que son principios, lo que les confiere un carácter habilitador del tratamiento. Esto implica que, para que se pueda llevar a cabo un tratamiento de datos, debe superarse un doble test, que consiste en superar los criterios de calidad enunciados en el artículo 6 y cumplir con lo que exige el artículo 7[565]. Además, esta regulación se completará con el cumplimiento del artículo 8 Directiva 95/46/CE, cuando lo que se quiera tratar sean categorías especiales de datos.

El artículo 7 Directiva 95/46/CE establece los supuestos que legitimarán el tratamiento de datos, de forma que lo que no esté incluido en estos supuestos debe entenderse como prohibido. Se trata de una lista cerrada por lo que, en este caso, los

[564] De hecho, así lo reconoce la misma Directiva 95/46/CE que en su Considerando 23 indica que "los Estados miembros están facultados para garantizar la protección de las personas tanto mediante una ley general relativa a la protección de las personas respecto del tratamiento de los datos de carácter personal como mediante leyes sectoriales, como las relativas a los institutos estadísticos".

[565] M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, pág. 110. También lo confirman la Sentencia del TJUE de 30 de mayo de 2013, *Worten*, C-342/12, EU:C:2013:355, apdo. 33, donde además remite a Sentencia del TJUE de 20 de mayo de 2003, *Rechnungshof/Österreichischer Rundfunk* y otros C-465/00, C-138/01 y C-139/01, EU:C:2003:294, apdo. 65; Sentencia del TJUE de 16 de diciembre de 2008, *Heinz Huber*, C-524/06, EU:C:2008:724, apdo 48, y Sentencia del TJUE de 24 de noviembre de 2011, *ASNEF, FECEMD/Administración del Estado*, C-468/10 y C-469/10, EU:C:2011:777, apdo. 26.

Estados miembros sólo pueden permitir el tratamiento de datos cuando se de alguno de estos supuestos habilitantes.

Los Estados miembros tampoco podrán añadir requisitos adicionales a los establecidos por este artículo en los diferentes supuestos previstos[566]. Así lo ha interpretado el TJUE, que consideró que la armonización perseguida por la Directiva 95/46/CE, no es una armonización de mínimos, sino una armonización completa[567]. Se trata, por lo tanto, de una armonización de máximos que establece un alto nivel de protección para los ciudadanos de su derecho a la protección de datos.

Por ello, aunque la Directiva 95/46/CE establezca que los Estados miembros deben precisar las condiciones en que son lícitos los tratamientos de datos personales, se fija como límite a esta libertad las disposiciones del Capítulo II de la Directiva, donde se encuentra el citado artículo 7 (art. 5 Directiva 95/46/CE)[568]. Los supuestos que permiten el tratamiento de datos personales son si:

> "a) el interesado da su consentimiento de forma inequívoca, o b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o[569] c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o d) si es necesario para proteger el interés vital del interesado[570], o e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos[571], o f) es necesario para la satisfacción del interés legítimo

[566] Sentencia del TJUE de 24 de noviembre de 2011, *ASNEF, FECEMD/Administración del Estado*, C-468/10 y C-469/10, EU:C:2011:777, apdos. 33-36, 95-99.
[567] Sentencia del TJUE de 6 de noviembre de 2003 *Bodil Lindqvist*, C-101/01, EU:C:2003:596, apdos. 95-96.
[568] El artículo 5 Directiva 95/46/CE viene soportado por los Considerandos 9 y 22 que establecen esta capacidad de los Estados miembros de precisar en su derecho nacional las condiciones generales de licitud del tratamiento de datos, aunque les instan a mejorar la protección que proporcionaba su legislación en el momento de aprobación de la directiva.
[569] La Ley húngara entiende que el requisito de consentimiento es necesario cuando se quiere ejecutar un contrato entre el interesado y el responsable (Secciones 5 y 6 Ley húngara).
[570] Respecto a este supuesto se ha incluido la legitimación para tratar datos en caso de catástrofes, con el fin de poder asistir a los damnificados (parágrafo 8.3.7 Ley austríaca). Algunas leyes han extendido la protección no sólo la integridad física, la vida del interesado, sino también sus propiedades (art. 2A.1.b.iv Ley irlandesa, Sección 6.2 Ley húngara, art. 9.b Ley checa-aunque en sede de datos sensibles-). El GA29, sin embargo, interpreta que tanto este supuesto, como el que establece el artículo 8.2.c) Directiva 95/46/CE para categorías especiales de datos, parece que deben interpretarse estrictamente y respecto cuestiones en las que se pone en peligro la vida de las personas, de acuerdo con el Considerando 31 Directiva 95/46/CE. *Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC, 844/14/EN WP 217, 9.4.2014, Article 29 Data Protection Working Party*, pág. 20.
[571] El Considerando 32 Directiva 95/46/CE especifica que corresponde a las legislaciones nacionales determinar si el responsable del tratamiento que tiene conferida una misión de interés públio o inherente al ejercicio del poder público, debe ser una administración pública u otra persona de derecho público o

perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección."

El análisis de estos supuestos de legitimación del tratamiento de datos se torna esencial. Antes de iniciar el tratamiento el responsable deberá escoger uno de los supuestos incluidos en la ley nacional que se le aplique y que, forzosamente, deben respetar el contenido de la regulación de la Directiva 95/46/CE. La elección debe adecuarse al tratamiento que quiera realizar y, si no pudiera encontrar el encaje en ninguna de estas bases jurídicas, no podría realizar el tratamiento.

Sin embargo, existen diferencias entre la regulación de la Directiva 95/46/CE y la de las leyes nacionales, especialmente en los supuestos referidos al consentimiento, el cumplimiento de una obligación jurídica y la satisfacción de un interés legítimo[572]. Estas divergencias han hecho que se tenga que pronunciar al respecto el TJUE que ha estimado que los supuestos del artículo 7, letras c), e) y f) Directiva 95/46/CE tienen efecto directo y, por tanto, podrán invocarlos los particulares ante los órganos jurisdiccionales nacionales para evitar la aplicación de normas de derecho interno contrarias a los mismos[573].

3.1.1. La elección del supuesto habilitante del tratamiento de datos

Todos los supuestos de legitimación de un tratamiento, excepto el primero (el consentimiento), se expresan como una necesidad para llevar a cabo una finalidad determinada (la ejecución de un contrato, la protección del interés vital del interesado, el cumplimiento de una misión de interés público o la satisfacción de un interés legítimo del responsable). El GA29 señala, por tanto, que estos preceptos requieren una "prueba de

privado y cita como ejemplo una asociación profesional. Respecto a esta base jurídica, el GA29 especifica que la misión de interés público o el poder público deben referirse a una autoridad de la Unión Europea o de un Estado miembro, no de un país tercero. *Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC, op. cit.*, pág. 21.

[572] *Commission Staff Working Paper, Impact assessment accompanying the document Regulation of the European Parliament […], op. cit., Annex 2*, pág. 27.

[573] Sentencia del TJUE de 20 de mayo de 2003, *Rechnungshof/Österreichischer Rundfunk* y otros C-465/00, C-138/01 y C-139/01, EU:C:2003:294, respecto al efecto directo del art. 7, letras c) y e) Directiva 95/46/CE y Sentencia del TJUE de 24 de noviembre de 2011, *ASNEF, FECEMD/Administración del Estado*, C-468/10 y C-469/10, EU:C:2011:777, respecto al efecto directo del artículo 7.f) Directiva 95/46/CE.

necesidad" que limitará el contexto en el que se podrán aplicar[574]. Además esta noción de necesidad ha sido considerada como un concepto autónomo y, por tanto, debe tenerse en cuenta que tendrá un significado a nivel comunitario, independiente del que puedan darle los ordenamientos nacionales[575].

El GA29 estima que el hecho de que los supuestos indicados requieran de esa "prueba de necesidad" no implica que el consentimiento permita mayor margen de maniobra[576]. El consentimiento aparece como una vía "fácil" y "segura" para garantizar una legitimación del tratamiento. No obstante, en ocasiones esta percepción puede ser equívoca y dar lugar a problemas prácticos[577]. El consentimiento debería ser un fundamento al que acudir si no se halla ninguna finalidad que justifique el tratamiento de

[574] Dictamen 15/2011, sobre la definición de consentimiento, 01197/11/ES WP187, 13.7.2011, Grupo de protección de datos del artículo 29, pág. 8 y *Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC, op. cit.*, pág.11.

[575] Sentencia del TJUE de 16 de diciembre de 2008, *Heinz Huber*, C-524/06, EU:C:2008:724. En esta sentencia, el señor Huber de nacionalidad austríaca se instaló en Alemania donde ejerció su actividad de agente de seguros. En Alemania se mantiene un Registro Central de Extranjeros referido sólo a ciudadanos extranjeros residentes en Alemania con el objetivo de controlar la residencia de estas personas, de forma que, entre otros datos, figuran las entradas y salidas del territorio. El señor Huber solicitó la cancelación de sus datos en este registro por considerarlo una medida discriminatoria respecto a los ciudadanos alemanes. Entre las cuestiones prejudiciales planteadas, se pregunta si es compatible este tratamiento de datos personales con el requisito de necesidad previsto en el artículo 7.e) Directiva 95/46/CE. El tribunal hace mención de su jurisprudencia sobre la armonización completa que persigue la Directiva 95/46/CE y en consecuencia, al pretender equiparar el nivel de protección entre los Estado miembros, el concepto de necesidad que establece el artículo 7.e) Directiva 95/46/CE que pretende delimitar uno de los supuestos en los que resulta lícito el tratamiento de datos no puede, según el tribunal tener un contenido variable en función de los Estados miembros. Por tanto, lo califica el tribunal de concepto autónomo del derecho comunitario. Si bien el TJUE deja en manos de los tribunales nacionales la decisión sobre si la normativa en litigio cumple este criterio de necesidad, con el fin de permitir a las autoridades competentes controlar el cumplimiento de la normativa referente a la residencia, no considera el tribunal que sea necesario, según esta disposición, que se traten estos datos con fines estadísticos.

[576] Así, por ejemplo, si se opta por el supuesto del artículo 7.b) Directiva 95/46/CE no basta que el tratamiento esté cubierto por la relación contractual, de forma que el responsable lo pueda haber previsto en el clausulado que se suscriba con el titular de los datos, sino que realmente debe ser necesario para la ejecución del contrato. Asimismo, el test de necesidad debe conectarse con el principio de limitación de finalidad, de forma que si se cita como ejemplo de nuevo el artículo 7.b) Directiva 95/46/CE, esta base jurídica sólo cubrirá los fines relativos a la ejecución normal del contrato. No cubriría por tanto, los fines conectados con posibles incidentes o conflictos como una posible demanda ante los tribunales por incumplimiento del contrato o como la gestión de cobro de la deuda por impago derivado también del contrato. En el caso del tratamiento relativo a las medidas precontractuales, el GA29 indica que la base jurídica sólo cubriría aquél que tuviera que realizarse en el marco de una solicitud del titular de los datos, no si la medida precontractual se realizara por iniciativa del responsable o de un tercero. Dictamen 15/2011 sobre la definición de consentimiento, *op. cit.*, pág. 8 y *Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC, op. cit.*, págs. 16 a 18.

[577] Si el responsable opta por la vía del consentimiento debe tener en cuenta la posibilidad obvia de que el interesado no acepte el tratamiento. En caso de que el responsable hubiera elegido mal el supuesto legitimador se encontraría también ante una situación que podría acarrearle dificultades. Además, como indica el GA29, en algunas situaciones no podrá considerarse válido el consentimiento otorgado. El responsable, por lo tanto, obtendrá una falsa sensación de seguridad que podrá quebrar en cualquier momento. Dictamen 15/2011 sobre la definición de consentimiento, *op. cit.*, págs. 14 a 16.

datos y que se contemple en los otros supuestos enumerados. En ocasiones, el responsable tendrá que buscar para el tratamiento de datos diversos supuestos que le legitimen, si por ejemplo, una parte de este tratamiento de datos se pudiera amparar en un contrato que tuviera con el interesado (art. 7.b Directiva 95/46/CE), pero otra parte del tratamiento no se pudiera situar en este supuesto[578].

Un criterio adicional que aporta el GA29 para saber si es posible optar o no por el consentimiento es el relativo a la naturaleza del responsable. Si el responsable es una entidad del sector público, lo normal es que opte por el supuesto legitimador del apartado c) o el e) del artículo 7 Directiva 95/46/CE, referidos al cumplimiento de una obligación jurídica o de una misión de interés público por parte del responsable del tratamiento, respectivamente[579].

3.1.2. La prevalencia de algunos supuestos en las leyes nacionales

La regulación que contiene el artículo 7 Directiva 95/46/CE sitúa a los supuestos de legitimación del tratamiento de datos en el mismo plano, sin otorgar mayor importancia a uno sobre el otro[580]. No sucede lo mismo en las leyes nacionales donde se da prevalencia en muchos casos a algunos de estos supuestos. Principalmente, se da mayor importancia al consentimiento y a la ley como supuestos habilitadores del tratamiento[581].

El principio del consentimiento se halla en la base de la fundamentación del derecho a la protección de datos como derecho a la autodeterminación informativa[582]. El

[578] *Ibídem*, pág. 8.
[579] *Ibídem*, págs. 15 a 17.
[580] Así lo ha entendido también el GA29 que indica que no hay ni jerarquía ni se debe otorgar ninguna relevancia al orden en el que se citan las bases jurídicas del artículo 7 Directiva 95/46/CE. *Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC op. cit.*, pág. 10.
[581] No obstante, cabe mencionar la regulación de la Ley austríaca, ya que su regulación gira entorno al concepto de interés legítimo (parágrafo 8.3 Ley austríaca).
[582] En referencia a la sentencia del Tribunal Constitucional Federal alemán sobre la Ley del censo de 1983, DENNINGER entiende que el derecho a la autodeterminación informativa protege la libertad de autodefinición del individuo. El tribunal alemán, comenta el autor, extrajo del derecho fundamental del libre desarrollo de la personalidad la competencia de cada individuo "de disponer principalmente sobre la revelación y el uso de sus datos personales" y, de esta manera, proteger su libertad de decisión. E. DENNINGER, "El derecho a la autodeterminación informativa", trad. cast. de A.E. PÉREZ LUÑO; A.E., PÉREZ LUÑO (Dir.), VVAA, *Problemas actuales de la documentación y la informática jurídica, Actas del*

consentimiento es la manifestación máxima del poder de control que tiene el interesado para permitir o no el tratamiento de datos efectuado por el responsable. Por eso, algunos ordenamientos nacionales, como el español, elevan al consentimiento por encima de otros supuestos de legitimación, de forma que éste supuesto es la regla general para tratar datos y los otros supuestos legitimadores son opciones de índole secundaria que tiene el responsable[583]. La configuración del derecho de protección de datos como un derecho de libertad, donde el poder de disposición de los datos es un poder positivo, implica que, en algunas de estas legislaciones nacionales, se de este papel preponderante al consentimiento.

De hecho, en algunas leyes nacionales esta prevalencia del consentimiento se lleva más allá, de forma que se entremezcla con los demás supuestos de legitimación para construir una regulación harto compleja, si se compara con la regulación tan simple de la Directiva 95/46/CE[584]. También se complica la regulación en las leyes nacionales que han optado por separar las disposiciones aplicables al sector público y al sector privado y que se refieren precisamente a los supuestos de legitimación del tratamiento de datos[585].

A continuación se analizan, por su especial problemática, los supuestos de legitimación consistentes en el consentimiento del interesado, el cumplimiento de una obligación jurídica y la satisfacción del interés legítimo.

Coloquio Internacional celebrado en la Universidad de Sevilla, 5 y 6 de marzo de 1986, Fundación Cultural Enrique Luño Peña, Madrid, 1987, pág. 272-273.

[583] Ver Capítulo VI respecto al ordenamiento español. Pueden citarse como ejemplos de la prevalencia del consentimiento las Leyes alemana, griega, checa, chipriota, estonia, húngara, italiana, croata y rumana.

[584] Secciones 5 y 6 Ley húngara.

[585] En la Ley italiana se establece la prevalencia del consentimiento pero únicamente para el sector privado. Y es que la regulación italiana distingue entre el sector público y el privado, de forma que, en lo que se refiere a la legitimación para tratar datos, cuando sea el sector público el que va a llevarlo a cabo, no precisará del consentimiento del afectado, siempre que se realice para desarrollar las funciones de la administración y limitado por la legislación aplicable (Sección 18 Ley italiana). En cambio, el tratamiento de datos personales que efectúe el sector privado y los *enti pubblici economici* exige como regla general el consentimiento expreso del afectado para que pueda llevarse a cabo (Sección 23 Ley italiana). Actualmente la Ley alemana mantiene la doble regulación para sector público y privado e incluye regulaciones diferenciadas de los supuestos legitimadores en ambas partes, aunque respecto a ambos sectores, en la parte que se dedica a las disposiciones generales se permite que se puedan tratar datos con el consentimiento de la persona (Sección 4.1 Ley alemana). Además, en la Ley alemana la regulación aún se complica más, ya que regula la legitimación para las diversas operaciones de tratamiento (recogida, almacenamiento, modificación, uso y comunicación). En la Ley eslovena también se diferencia entre la legitimación de los tratamientos, dependiendo de si los lleva a cabo el sector público o privado, pero establece en un apartado de aplicación general la prevalencia de la ley y el consentimiento como supuestos habilitantes para el tratamiento de datos personales (art. 8.1 Ley eslovena). Después regula por separado los diferentes supuestos de legitimación aplicables a ambos sectores (art. 9 para el sector público y art. 10 para el sector privado, Ley eslovena).

3.1.3. El consentimiento del interesado

Para analizar las características del consentimiento como opción legitimadora del tratamiento de datos, además de lo establecido en el artículo 7.a) Directiva 95/46/CE, que indica que el interesado debe dar su consentimiento de forma inequívoca, hay que acudir a su definición: "consentimiento del interesado: toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan" (art. 2.h) Directiva 95/46/CE). Aunque no se haga referencia al momento en el que debe otorgarse el consentimiento, al ser un supuesto habilitante del tratamiento de datos, es natural que deba ser previo al tratamiento como regla general[586].

La mención a "toda manifestación de voluntad" y la palabra "consienta" implica para el GA29 que el interesado debe realizar una acción positiva para poder considerar que consiente[587]. En consecuencia, quedaría en duda si se admite como forma de otorgar el consentimiento la ausencia de una acción o incluso una acción pasiva, de forma que pueda interpretarse que, de todas formas, ha existido una "manifestación". Es decir, se admitiría el consentimiento llamado expreso, pero quedaría en duda la validez del consentimiento tácito[588].

La palabra "libre" implica para el GA29 que no deben existir consecuencias negativas si el interesado decide no otorgar su consentimiento[589]. Para poder determinar si el consentimiento es libre deben analizarse, según el GA29, todos los elementos que pudieran tener una influencia en la libertad del titular para elegir[590].

---

[586] Así lo deduce el GA29 que además hace mención a que en la versión alemana de la Directiva 95/46/CE y en la Ley alemana se utiliza el concepto de *Einwilligung,* definido en el Código civil alemán como aceptación previa. Dictamen 15/2011 sobre la definición de consentimiento, *op. cit.*, pág. 11, nota 13.

[587] *Ibídem,* págs. 13 a 14.

[588] Hay leyes nacionales como la búlgara (art. 4.1.2 Ley búlgara), la estonia, la italiana que exigen el consentimiento expreso. En caso de la Ley italiana hay que recordar que el supuesto de legitimación por vía de consentimiento sólo se establece para el sector privado (Sección 23 Ley italiana). La Ley estonia regula de forma pormenorizada los requisitos del consentimiento y no admite el consentimiento tácito (art. 12 Ley estonia). En el lado contrario, la LOPD, como se examinará posteriormente, admite claramente el consentimiento tácito y además regula un procedimiento específico para recogerlo (art. 14 RLOPD).

[589] La Ley de Liechtenstein define el consentimiento como una declaración de intenciones otorgada sin coacción (art. 3.1.m Ley Liechtenstein).

[590] Como ejemplo el GA29 menciona el caso de los empleados, en el que el empleador ostenta una situación de superioridad sobre el empleado que puede ver peligrar su puesto o sus condiciones laborales si rechaza el

La palabra "específico" alude a la granularidad del consentimiento que debe otorgarse respecto a cada uno de los diferentes aspectos del tratamiento de datos, claramente identificados. Además, el consentimiento deberá referirse al tratamiento de datos personales que sea razonable y necesario respecto a la finalidad perseguida, por lo que no puede cubrir todos los usos[591].

El consentimiento debe ser "informado", ya que para asegurar el control de los datos por parte del titular de los mismos, es imprescindible que éste conozca que se va a llevar a cabo el tratamiento, para que pueda consentir. De esta forma, el consentimiento irá ligado a la obligación de informar (arts. 10 y 11 Directiva 95/46/CE). La información debe cumplir, según el GA29, con requisitos de calidad, de forma que el texto debe ser simple y comprensible para un usuario. Además debe ser accesible y visible, no siendo suficiente que la información esté disponible en algún sitio, sino que debe proporcionarse directamente al afectado[592].

Otro requisito que establece la Directiva 95/46/CE es que el consentimiento debe ser "inequívoco" (art. 7.a Directiva 95/46/CE). Para el GA29 esto implica que no debe haber dudas sobre la intención del sujeto de consentir, no cabe la ambigüedad respecto a la manifestación de voluntad. Para ello, será necesario que los responsables del tratamiento creen procedimientos robustos de solicitud de consentimiento, ya sea porque se recoja expresamente, o porque se utilizan procedimientos que permiten deducir claramente la obtención del mismo.

El GA29 resalta la importancia de que el responsable pueda acreditar el consentimiento otorgado[593]. En este sentido, en algunas leyes nacionales se establece la presunción de que, en caso de dudas sobre si se ha otorgado el consentimiento se deberá

---

tratamiento de datos personales. También cita, como ejemplo, el del escáner corporal de los aeropuertos, de forma que entiende que el miedo a las consecuencias negativas que podría conllevar el hecho de negarse al uso de los mismos hace que no pueda admitirse el consentimiento y que deba legitimarse por ley su utilización. Dictamen 15/2011 sobre la definición de consentimiento, *op. cit.*, págs. 14 a 16.

[591] *Ibídem*, págs. 19 a 20.

[592] *Ibídem*, págs. 21 a 22. Además hacer mención a las Leyes estonia y checa que regulan la obligación de informar conectada con el consentimiento y establecen el contenido de esta información (art. 12 Ley estonia y art. 5.4 Ley checa).

[593] *Ibídem*, pág. 24. En este sentido indicar que la Ley alemana establece que el consentimiento debe darse principalmente por escrito (art. 4a Ley alemana).

entender que no se ha otorgado[594]. Asimismo, el GA29 también demanda del responsable que cuanto más complicado sea el tratamiento de datos, más se debe esperar de su actuación al solicitar el consentimiento. Es decir, cuanto más difícil sea para un ciudadano medio entenderlo, más esfuerzos debe hacer el responsable para demostrar que informó correctamente cuando solicitó el consentimiento[595].

Respecto a la validez del consentimiento, el GA29 entiende que se encuentra implícita en la Directiva 95/46/CE la capacidad de retirarlo[596].

3.1.4. El cumplimiento de una obligación jurídica

Este supuesto pretende dar cabida a aquellos tratamientos que debe realizar el responsable del tratamiento en cumplimiento de una obligación legal[597]. Por tanto, se trata de un supuesto ampliamente utilizado. Sin embargo, debe tenerse en cuenta que no toda obligación legal permitirá realizar un tratamiento amparado en este supuesto, sino que deberá cumplirse lo que establece el artículo 52.1 Carta UE respecto a los límites a los derechos contemplados en la misma[598].

Esta disposición establece que cualquier limitación al derecho a la protección de datos establecido en su artículo 8 Carta UE es necesario que esté establecida en una ley. Sin embargo, esto no es suficiente. Además debe respetarse el contenido esencial del derecho y el principio de proporcionalidad. Este principio obliga a que se realice una

[594] Sección 6 Ley húngara, artículo 12 Ley estonia, artículo 5.4 Ley checa.
[595] Dictamen 15/2011 sobre la definición de consentimiento, *op. cit.*, pág. 28
[596] Aunque el GA29 considera que sí se encuentra la posibilidad de retirar el consentimiento, sin efectos retroactivos, en los artículos 6.3 y 9, apartados 3 y 4 Directiva 2002/58/CE, *Ibídem*, pág. 37. Las Leyes croata y estonia permiten la revocación del consentimiento, aunque la croata sólo en algunos supuestos (art. 7 Ley croata), mientras que la estonia no se limita, aunque si no se revoca, establece un plazo de validez para el consentimiento que se refiere a la vida del interesado y treinta años más después de su muerte (art. 12 Ley estonia). La legislación española también contempla el derecho a revocar el consentimiento por causa justificada y sin efectos retroactivos (art. 6.2 LOPD y art. 17 RLOPD).
[597] Y es que la referencia a obligación "jurídica" responde a la traducción del término "legal" en inglés que puede traducirse como jurídica o legal, indistintamente. En este sentido en el Considerando 30 se hace referencia a "la observancia de una obligación legal".
[598] Esta disposición indica que "Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás" (art. 52.1 Carta UE). KUNER indica que no toda obligación legal permitirá al responsable realizar el tratamiento de datos, sino que las leyes que contengan estas obligaciones deberán ser legítimas y proporcionadas. C. KUNER, *European data protection law, corporate compliance and regulation*, *op. cit.*, pág. 76.

ponderación y sólo se introduzcan en las leyes aquellas limitaciones que sean necesarias y respondan a objetivos de interés general reconocidos por la UE o respondan a la necesidad de proteger los derechos y libertades de otros ciudadanos.

Así, el TJUE, en aplicación de este artículo ha considerado en los asuntos *Eifert* y *Schwarz*, que un reglamento europeo es una ley susceptible de incorporar limitaciones al derecho a la protección de datos cuando se persiga el principio de transparencia establecido en los tratados de la UE o se persiga evitar la entrada ilegal de personas en el territorio de la UE. Al analizar si estas limitaciones cumplen con el resto de requisitos, el tribunal invalida los artículos discutidos en el caso *Eifert*[599] y, por el contrario, estima procedentes las disposiciones en litigio en el asunto *Schwartz*[600]. También hay que

[599] El TJUE, en respuesta a una cuestión prejudicial por el *Verwaltungsgericht Wiesbaden* (Alemania), consideró que la publicación, en un sitio web de los datos nominales de los beneficiarios de ayudas del FEAGA y del FEADER y de los importes específicos percibidos por ellos, constituía una injerencia en su vida privada, a efectos del artículo 7 Carta UE y en su derecho a la protección de datos, establecido en el artículo 8 de la Carta UE. Al analizar si esta injerencia cumplía con lo establecido en el artículo 52.1 Carta UE manifestaba que esta publicación la ordenaba un reglamento europeo y que se perseguía el principio de transparencia recogido en los artículos 1 y 10 TUE y en el artículo 15 TFUE. Sin embargo, al analizar el principio de proporcionalidad, el tribunal consideró que, al adoptar el artículo controvertido, el Consejo y la Comisión no tomaron en consideración otras formas de publicación de la información que podían respetar el objetivo perseguido y que podían ser menos lesivas para los derechos de tales beneficiarios. Por tanto, el tribunal invalida los artículos controvertidos por no haberse respetado en su adopción el principio de proporcionalidad. Hay que decir que, pese a que cita la Directiva 95/46/CE y las posibles bases jurídicas aplicables para legitimar el tratamiento, no la menciona en la argumentación. El TJUE acude directamente a la Carta UE que, además, a partir del Tratado de Lisboa, podrá utilizar pese que no fuera aplicable la Directiva 95/46/CE. Sentencia del TJUE de 9 de noviembre de 2010, *Vloker und Markus Schecke GbR, Hartmut Eifert*, C-92/09 y C-93/09, EU:C:2010:662.

[600] Otro ejemplo de aplicación de la doctrina relativa a la limitación de derechos es una sentencia del TJUE en la que analizó la validez de un precepto del Reglamento (CE) nº2252/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros. De nuevo sólo cita la Directiva 95/46/CE a la que remite el Reglamento en cuestión y se menciona como posible base jurídica la del artículo 7.e) Directiva 95/46/CE, relativa al cumplimiento de una misión de interés público. No obstante, creo que ilustra bien la aplicación de la limitación de derechos. La sentencia respondía a una cuestión prejudicial que solicitaba el *Verwaltungsgericht Gelsenkirchen* (Alemania), en el marco de un procedimiento en el que el Sr. *Schwarz* se había negado a que le tomaran sus huellas dactilares para expedirle un pasaporte, porque entendió que se vulneraba su derecho a la protección de datos. El tribunal acudió al artículo 8.2 Carta UE, según el que sólo pueden ser tratados los datos personales con el consentimiento del interesado o en virtud de otro fundamento legítimo previsto por ley. Según recuerda el tribunal, los artículos 7 y 8 Carta UE no constituyen prerrogativas absolutas, sino que deben ser considerados respecto a su función en la sociedad. Como el tratamiento de las huellas dactilares se efectuó en virtud del Reglamento europeo mencionado procedía, por tanto, en la medida que suponía una limitación al derecho de protección de datos, la aplicación del artículo 52.1 Carta UE. El TJUE realizó el análisis del artículo controvertido y llegó a la conclusión de que cumplía con los requisitos establecidos en el artículo 52.1 Carta UE. En este sentido, consideró que la limitación a los derechos estaba prevista en una ley, al ser incluida en un reglamento europeo. La limitación perseguía el interés general, ya que pretendía prevenir la falsificación de pasaportes e impedir su uso fraudulento por personas que no sean su legítimo titular y, por tanto, evitar la entrada ilegal de personas en el territorio de la UE. No había nada que permitiera deducir que no se respetaba el contenido esencial de los derechos. Al examinar si la limitación era proporcionada, con respecto al objetivo perseguido, se examinó la regulación y se estableció que la conservación de impresiones dactilares prevista

recordar la importante jurisprudencia del TEDH sobre la limitación de derechos en referencia al derecho a la vida privada del artículo 8 CEDH, donde se incardina el derecho a la protección de datos[601].

El GA29 ha indicado que la obligación jurídica debe hallarse en una ley de la UE o de sus Estados miembros[602]. No podría utilizarse una obligación jurídica incorporada en leyes de terceros países, a no ser que esta obligación se hubiera incorporado en el ordenamiento del Estado miembro, por ejemplo, a través de un convenio internacional. En todo caso, podría acudirse, como sugiere el GA29, a otra base jurídica, como la de satisfacer un interés legítimo del responsable o de un tercero[603].

Respecto a las obligaciones legales y también a la noción de misión de interés público o inherente al ejercicio del poder público (art. 7.e) Directiva 95/46/CE), la Comisión Europea ha alertado sobre los problemas que las diferencias en las legislaciones pueden originar para tratamientos de datos que se desarrollan en más de un Estado miembro[604].

---

en un dispositivo dotado de fuertes medidas de seguridad reducía el riesgo de falsificación. Ante la alegación de los posibles errores en ese método de verificación, el tribunal consideró que ello no es determinante, ya que bastaba con que redujera el riesgo existente. Además se indicó que la falta de concordancia de las impresiones dactilares con el poseedor del pasaporte no implicaba la denegación automática de la entrada al territorio, sino que conllevaría un control de las autoridades competentes. Por tanto, el TJUE concluyó que era un mecanismo idóneo para la finalidad perseguida. Sentencia del TJUE de 17 de octubre de 2013, *Schwarz*, C-291/12, EU:C:2013:670, apdos. 33 ss.

[601] Como ejemplo se puede citar una sentencia en la que se valoraba si era posible la conservación por las autoridades policiales de muestras de tejido, perfiles de ADN y huellas dactilares recogidas en el marco de una investigación, de los recurrentes sospechosos pero, finalmente, no condenados por el delito investigado. El TEDH considera que existe violación del artículo 8 CEDH, ya que estima que pese a estar previto en una ley y responder a un fin legítimo, no sería necesario en una sociedad democrática. No existe, según el tribunal una necesidad social ni es proporcionada la medida respecto al fin perseguido. Así, recuerda el tribunal que el Convenio 108 establece que los datos deben ser adecuados y no excesivos respecto al fin perseguido y sólo se pueden conservar de forma que identifiquen a los sujetos mientras dure la finalidad para la que se registraron. El Tribunal destaca que los datos se conservan sin tener en cuenta la gravedad del delito investigado y sin distinguir entre condenados o no, lo que conlleva un peligro de estigmatización. Sentencia del TEDH de 4 de diciembre de 2008, *S. and Marper v. The United Kingdom*, apdos. 103-126.

[602] *Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC, op. cit.*, pág. 19.

[603] Aunque en este caso, deberán respetarse los requisitos que establece esa base jurídica para su correcta aplicación, *Ibídem*.

[604] *Commission Staff Working Paper, Impact assessment accompanying the document Regulation of the European Parliament […], op. cit., Annex 2*, pág. 27.

3.1.5. La satisfacción del interés legítimo

El artículo 7.f) Directiva 95/46/CE establece dos requisitos acumulativos para entender que el tratamiento de datos es lícito. El primero es que el tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero al que se comuniquen los datos y el segundo es que no prevalezcan los intereses, derechos y libertades fundamentales del interesado.

Por lo tanto, esta regulación exige una ponderación de los derechos e intereses en conflicto que dependerá del caso concreto. Por esta razón, este requisito se conoce como el test del equilibrio o ponderación de intereses (*balance of interest*). En un lado de la balanza está el interés del responsable del tratamiento y en el otro el interés o los derechos del interesado[605]. En caso de que el responsable tuviera dudas acerca de qué es lo que pesa más en la balanza, aún podrá incluir medidas adicionales que vayan más allá del mero cumplimiento de lo establecido en la Directiva 95/46/CE, de forma que consiga contrarrestar el posible impacto negativo del tratamiento en los intereses o derechos del interesado[606].

Una medida que la misma Directiva 95/46/CE establece, como garantía adicional, para el caso de que el responsable escoja este supuesto, es el derecho de oposición (art. 14.a y Considerando 30 Directiva 95/46/CE[607].

La determinación de lo que debe considerarse un interés legítimo prevalente se deja a los Estados miembros, aunque se enmarca en el desempeño de la gestión ordinaria

[605] El GA29 enlaza esta protección general de los derechos fundamentales y los intereses de los titulares de datos con el artículo 1.1 Directiva 95/46/CE, que establece, como objeto de la misma, la protección de las libertades y de los derechos fundamentales de las personas físicas en general, aunque luego indique que protege en particular el derecho a la intimidad en lo que respecta al tratamiento de los datos personales. *Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC, op. cit.*, pág. 4.

[606] El GA29 describe la metodología a seguir en este anális en su *Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC op. cit.*, págs. 37 a 43.

[607] El derecho de oposición está previsto de forma específica para las bases jurídicas establecidas en el artículo 7, apartados e) y f) con la condición de que el interesado tenga razones legítimas, que provengan de su situación particular, que justifiquen esta oposición. De esta forma, tal como indica el GA29, en el caso de la base jurídica referida al interés legítimo, el responsable del tratamiento, en caso de que el interesado ejerciera este derecho de oposición debería volver a realizar la ponderación, ante estas nuevas circunstancias para ver si, esta vez, la balanza se inclina a favor del interesado. *Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC op. cit.*, pág. 45.

de empresas y otras entidades (Considerando 30 Directiva 95/46/CE)[608]. Es decir, la finalidad de este supuesto va en la dirección de permitir el funcionamiento de las actividades empresariales o de las administraciones públicas.

Hay que entender que el objetivo de la Directiva 95/46/CE es asegurar la libre circulación de los datos personales en el mercado interior de la UE, mediante el logro de un grado de protección de los derechos fundamentales elevado en todos los Estados miembros. Por lo tanto, este apartado f) ampara aquellos supuestos que no se puedan anclar en los supuestos anteriores y que serán necesarios para lograr que se asegure una competencia efectiva[609]. Se mencionan, como ejemplos de lo que puede considerarse supuestos que entren dentro de esta previsión, las comunicaciones de datos a terceros con fines de prospección comercial o de prospección realizada por instituciones benéficas u otras asociaciones o fundaciones de carácter político[610].

El GA29 define este interés legítimo como el beneficio que persigue el responsable con el tratamiento, en contraste con el concepto de finalidad del tratamiento, que sería la razón concreta por la que se tratan los datos. Este interés debe ser lícito,

[608] Durante el proceso de elaboración de la Directiva 95/46/CE se añadió en la Propuesta de directiva de 1992 además del interés legítimo del responsable del tratamiento y del tercero a quien se comunican los datos, como intereses que podían prevalecer sobre el de los interesados, el interés general, que finalmente se eliminó del texto final. M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, págs. 112 a 113.

[609] Durante la elaboración de la Directiva 95/46/CE, la doctrina francesa, según apunta HEREDERO HIGUERAS, calificó este apartado f) del artículo 7 de disposión escoba (*disposition balai*) por englobar todos los supuestos que no se podían comprender en los apartados anteriores. *Ibídem*. Sin embargo, también hay que decir que no está de acuerdo con esta interpretación el GA29, que considera, que este supuesto no debería utilizarse como último recurso, cuando no se pudieran utilizar los otros supuestos. *Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC op. cit.*, pág. 3.

[610] Entiende HEREDERO HIGUERAS que el Considerando 30 Directiva 95/46/CE cita, a título indicativo, los tratamientos con fines de prospección comercial, benéficos o políticos. A esto añade que, al remitir el último inciso del artículo 7.f) Directiva 95/46/CE al artículo 1.1 Directiva 95/46/CE, que establece el principio de la libre circulación de los datos, se puede concluir que para determinar si el tratamiento es lícito deberán tenerse en cuenta los intereses del mercado, la competencia leal y la libre circulación de los datos en el mercado interior. Estos aspectos permitirán admitir como lícitos los tratamientos que sirvan de instrumento a actividades mercantiles como puede ser la evaluación de la solvencia. M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, págs. 112 a 113. El GA29 menciona como ejemplos de supuestos en los que *a priori* se podría hablar de que el responsable tiene un interés legítimo los siguientes: ejercicio del derecho a la libertad de expresión o información; marketing, publicidad; mensajes no solicitados no comerciales, como campañas políticas o búsqueda de donaciones; reclamaciones incluida la gestión de cobro; prevención de fraude, mal uso de servicios, blanqueo de capitales; sistemas de denuncia; seguridad física, tecnológica y seguridad de redes; los fines históricos científicos y estadísticos; la investigación (incluida investigación en materia de marketing). *Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC op. cit.*, pág. 25

suficientemente claro para poder articular la ponderación con los intereses y derechos del titular de los datos y además real y actual[611].

Hay que recordar el caso *SWIFT*, la empresa de mensajería financiera que proporcionó durante años información a las autoridades estadounidenses sobre las transacciones que gestionaba. Si bien el GA29 consideró inicialmente que podía tener un interés legítimo en cumplir con las citaciones (*subpoenas*) de la legislación estadounidense ya que, en caso contrario, podía ser sancionada, estimó, finalmente, que ello no podía prevalecer sobre el interés o los derechos y libertades fundamentales de los numerosos interesados afectados[612].

3.2. Categorías especiales de tratamientos

En caso de que el responsable quisiera llevar a cabo un tratamiento de datos personales que revelara el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como datos relativos a la salud o a la sexualidad, deberá cumplir con la regulación específica, que se encuentra en el artículo 8 Directiva 95/46/CE, que impone a los Estados miembros la obligación de prohibir, por regla general, este tipo de tratamientos de datos. Este reforzamiento de la protección para estos datos halla su justificación en su especial naturaleza, más proclive a dañar las libertades fundamentales, el derecho a la intimidad o el derecho a la vida privada de las personas[613]. No obstante, la prohibición general de tratamiento está excepcionada por los supuestos que se enumeran en los apartados 2, 3 y 4 artículo 8 Directiva 95/46/CE[614].

---

[611] El GA29 interpreta que el interés será lícito cuando esté de acuerdo con alguna ley, aunque interpreta de forma muy amplia lo que incluye en el término ley (cualquier tipo de normativa, jurisprudencia, derechos fundamentales, códigos de conducta, contratos, etc.). Cuando establece que el interés debe ser real y actual, el GA29 se refiere a que no puede ser un interés especulativo. *Ibídem*.

[612] Dictamen 10/2006 sobre el tratamiento de datos personales por parte de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (*Worldwide Interbank Financial Telecommunication*-SWIFT), *op. cit.*, págs. 8, 21 a 22.

[613] Considerandos 33 y 34 Directiva 95/46/CE. El derecho a la protección de datos se configura como un derecho instrumental que permite también la protección de otros derechos, como puede ser el derecho a la igualdad, de forma que a través del uso de estos datos especialmente sensibles se eviten discriminaciones. Precisamente, la autoridad de control inglesa estima que debe presumirse que estos datos especiales podrían utilizarse de forma discriminatoria por lo que precisan un refuerzo de la protección. *The guide to data protection, op. cit*, pág. 24

[614] Estos supuestos son los siguientes: si el interesado da su consentimiento explícito, aunque se posibilita que los Estados miembros establezcan que no sea posible que sirva de excepción este consentimiento; si el tratamiento es necesario para respetar las obligaciones y derechos del responsable del tratamiento en materia de derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea las garantías adecuadas; si el tratamiento es necesario para salvaguardar el interés vital del interesado o de otra persona si

Hay una diferenciación entre los datos, de forma que, respecto al origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas y la pertenencia a sindicatos, se debe prohibir el tratamiento de datos que revelen esta información. En cambio, en el caso de la salud y la sexualidad, lo que se debe prohibir es el tratamiento de datos relativos a estos aspectos, no que revelen estos aspectos. En consecuencia, el alcance del concepto de datos sensibles es más amplio cuando los datos se refieren, en general, a la ideología o al pensamiento, así como al origen racial o étnico, que cuando se refieren a aspectos como la salud o la sexualidad[615].

Hay que hacer referencia también al artículo 8.5 Directiva 95/46/CE que alude, aparentemente, al tratamiento de otra categoría de datos diferente de las enunciadas en el apartado 1[616]: los datos relativos a infracciones, condenas penales o medidas de

---

estuviera incapacitado para dar su consentimiento; si el tratamiento se efectúa por una fundación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en el curso de sus actividades legítimas y con las debidas garantías, siempre que se refiera a sus miembros o a las personas que mantengan contactos regulares con esta entidad por razón de su finalidad y además se limita la comunicación a terceros de los datos que no podrá realizarse sin consentimiento del interesado; si el tratamiento se refiere a datos que el interesado haya hecho manifiestamente públicos o sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial; si el tratamiento es necesario para la asistencia sanitaria siempre que lo realice un profesional sanitario sujeto al secreto profesional o por una persona sujeta a una obligación equivalente de secreto. Asimismo, los Estados miembros podrán establecer otras excepciones por motivos de interés público.

[615] En la Ley inglesa no se establece la regla general que proclama la directiva de prohibición del tratamiento de este tipo de datos. Asimismo, en esta ley se ha sustituido "datos personales que revelen" por "datos personales consistentes en información de" ("*personal data consisting of information as to*", Sección 2 Ley inglesa). El legislador inglés restringió así el concepto de datos sensibles ("*sensitive personal data*") ya que no es lo mismo un dato que es una información de las convicciones religiosas de alguien, que un dato que revela estas convicciones religiosas. D. s, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Contract _r: JLS/2008/C4/011 – 30-CE-0219363/00-28, Country Studies, A.6-United Kingdom, LRDP KANTOR Ltd & Centre for Public Reform, European Commission, Directorate General Justice, Freedom and Security, June 2010*, pág. 27, 31. Sin embargo, la autoridad de control inglesa interpreta la ley, de forma que aunque no considera que, el hecho de que el nombre de una persona denote su etnia o su religión, convierta este nombre en un dato sensible, si el tratamiento de ese dato se realizara, precisamente por esta información que revela, entonces sí se tendría que considerar que se tratan datos sensibles. *The guide to data protection*, *op. cit*, pág. 24.

[616] Y es que en el artículo 8.6 Directiva 95/46/CE se especifica que "las excepciones a las disposiciones del apartado 1 que establecen los apartados 4 y 5 se notificarán a la Comisión". Por lo tanto, se trata al artículo 8.5 Directiva 95/46/CE como una excepción a la prohibición de tratar los datos enunciada en el artículo 8.1 Directiva 95/46/CE. Esto plantea la cuestión de si hay que entender que sólo los datos mencionados en el artículo 8.1 Directiva 95/46/CE son susceptibles de ser prohibidos y excepcionados. De esta forma, en el artículo 8.5 Directiva 95/46/CE no se regularían los datos relativos a infracciones, condenas penales, medidas de seguridad, sanciones administrativas y procesos civiles, considerados independientemente, sino cuando se conecten con los datos relacionados en el artículo 8.1 Directiva 95/46/CE. No obstante, las legislaciones nacionales no han seguido esta interpretación, sino que han considerado estos datos de forma independiente.Como ejemplo baste citar la Ley belga que prohíbe el tratamiento de los datos relativos a litigios sometidos a órganos jurisdiccionales y administrativos, sospechas, investigaciones o condenas relativas a infracciones o sanciones administrativas o medidas de seguridad, con algunas excepciones (art. 8 Ley belga). En esta ley las excepciones son amplias ya que se ha intentado cubrir todos los posibles

seguridad, sanciones administrativas y procesos civiles. Se establecen dos opciones para poder tratar estos datos: que se realice bajo el control de una autoridad pública o que se prevean garantías en el derecho nacional[617]. No obstante, se precisa que el registro completo de condenas penales sólo se podrá llevar bajo el control de los poderes públicos y se deja al arbitrio de los Estados miembros la decisión de sujetar, también al control de los poderes públicos, el tratamiento de datos relativos a sanciones administrativas o procesos civiles.

En definitiva, en caso de que el responsable quiera realizar alguno de estos tratamientos especiales, tendrá que poder encajar el supuesto en una de las excepciones contempladas en el artículo 8 Directiva 95/46/CE. Sin embargo, aunque el responsable pueda incluir el tratamiento dentro de alguna de estas excepciones, esto no será suficiente. El hecho de incluir el tratamiento en una de estas excepciones significará que el tratamiento no estará prohibido, pero, aún faltará encontrar algún supuesto habilitante general, de los establecidos en el artículo 7 Directiva 95/46/CE. Una interpretación diferente podría arrojar que se debilitara, en realidad, la protección que se entiende reforzada para este tipo de datos[618].

---

tratamientos que se efectúan con estos datos, como aquellos que deben llevar a cabo los abogados para la defensa de sus clientes.

[617] El Reino Unido parece haber optado por la segunda opción de establecer garantías, ya que ha incluido este tipo de datos (datos relativos a la comisión o presunta comisión por el interesado de cualquier infracción, o los datos sobre cualquier procedimiento por cualquier infracción cometida o presuntamente cometida por él, el desarrollo de estos procedimientos o la sentencia de cualquier tribunal en estos procedimientos) en la definición de "datos personales sensibles", junto a las otras categorías especiales de datos (art. 2. g y h Ley inglesa). Al incluir este tipo de datos en la categoría de datos sensibles, sin diferenciarlos de todos los demás, la Ley inglesa les aplica el mismo régimen. Así, por ejemplo, una organización puede tratar este tipo de datos si obtiene el consentimiento del interesado. Cabe plantear, por tanto, si se han establecido las garantías que requiere la directiva. En entornos laborales, esta cuestión planteó problemas en el Reino Unido, ya que se generalizó la práctica de obligar a los candidatos a algún puesto de trabajo a ejercer un derecho de acceso a los registros policiales con el fin de poder ofrecer la información sobre los antecedentes penales. Actualmente esta conducta se ha tipificado como una infracción penal. A cambio se ha creado el *Criminal Records Bureau* que da soporte a las organizaciones para que puedan contratar de forma segura. Así lo pone de manifiesto D. KORFF, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Contract _r: JLS/2008/C4/011 – 30-CE-0219363/00-28, Country Studies, A.6-United Kingdom, op. cit.*, págs. 34 a 35.

[618] De esta forma, si se trataran los supuestos del artículo 8 Directiva 95/46/CE como supuestos habilitadores independientes de los establecidos en el artículo 7 Directiva 95/46/CE podría llegarse, por ejemplo, a una situación en la que se permitiera a un responsable tratar datos de ideología que el interesado haya hecho manifiestamente públicos y que no pudiera tratar sus datos referentes al domicilio hechos también manifiestamente públicos. Así lo ha confirmado el GA29, *Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC, op. cit.*, pág. 15.

Con relación al tratamiento de datos personales con fines periodísticos o de expresión artística o literaria, la Directiva 95/46/CE permite a los Estados miembros adoptar exenciones y excepciones en su la regulación en función de la ponderación entre los derechos fundamentales de libertad de expresión y libertad de información, como derecho a recibir y comunicar información, y el derecho a la protección de datos (art. 9 y Considerando 37 Directiva 95/46/CE).

Por último, hay que mencionar la referencia de la Directiva 95/46/CE al número nacional de identificación (art. 9.7 Directiva 95/46/CE). Este es un punto controvertido ya que en algunos países se consideró como una amenaza grave a los derechos de la persona y se llegó a prohibir su establecimiento[619]. La Directiva 95/46/CE deja libertad a los Estados miembros para que determinen las condiciones en las que podrá ser objeto de tratamiento este número nacional de identificación o cualquier otro medio de identificación de carácter general. Por lo tanto, los responsables que deban tratar este dato deberán acudir a la normativa nacional que lo regule[620].

Como ha resaltado la Comisión Europea, existen importantes diferencias entre las regulaciones nacionales y la Directiva 95/46/CE, en lo que respecta a estos tratamientos especiales de datos[621]. En algunas leyes nacionales se han añadido otras tipologías de datos a la lista del artículo 8 Directiva 95/46/CE[622] o se ha reforzado la protección otorgada[623].

---

[619] Como en la Constitución portuguesa que en el artículo 35.5 prohibe la asignación de un número de identificación único a los ciudadanos.

[620] En algunos casos se han previsto limitaciones al tratamiento de este tipo de datos como en el artículo 20 Ley eslovena, artículo 7 Ley lituana, artículo 13 Ley finlandesa, artículo 13 Ley letona, artículo 18 Ley maltesa, artículo 12 Ley noruega, Parte II del Anexo 1 Ley inglesa, artículo 11 Ley danesa, artículo 28 Ley polaca, artículo 6.2 Ley chipriota.

[621] *Commission Staff Working Paper, Impact assessment accompanying the document Regulation of the European Parliament […], op. cit., Annex 2,* págs. 28 a 30.

[622] En algunas leyes se añaden también en esta regulación con una protección más reforzada los datos genéticos (art. 7.1 Ley portuguesa, art. 6.1 Ley luxemburguesa, art. 4.2.4 Ley estonia, el art. 5.1.3 especifica el dato del genoma humano, art. 27 Ley polaca, art. 2.8 Ley islandesa), los datos relativos a los servicios sociales (art. 11.6 Ley finlandesa, o datos de problemas sociales graves como se refiere el art. 8 Ley danesa, art. 3.1.3.cc Ley de Liechtenstein), los datos relativos a la vida privada (art. 7.1 Ley portuguesa y art. 8 Ley danesa), la orientación erótica (art. 2 Ley chipriota) y también se alude específicamente a los datos relativos a las preferencias sexuales (art. 11.5 Ley finlandesa, art. 2.8 Ley islandesa que se refiere al comportamiento sexual), datos biométricos (art. 4.2.5 Ley estonia, art. 4.b Ley checa), las adicciones (art. 27 Ley polaca, art. 3.3.b Ley húngara, el art. 2.8 Ley islandesa que hace referencia al consumo de alcohol, medicamentos y narcóticos), los datos que revelen la nacionalidad (art. 4.b Ley checa). La Ley de Liechtenstein además, aunque no considera que sean datos sensibles, brinda la misma protección que tienen este tipo de datos a los datos relativos a los perfiles personales. La ley define este tipo de datos como

3.3. La obligación de informar

La obligación de informar al interesado se ubica en el Capítulo II Directiva 95/46/CE, entre las condiciones generales para la licitud del tratamiento de datos personales. Este requisito se sitúa en el momento inicial del ciclo del dato, cuando éste se introduce en el sistema de información del responsable. La Directiva 95/46/CE se refiere, concretamente, al responsable del tratamiento como sujeto obligado[624], aunque también añade a su representante[625].

El deber de informar persigue que el tratamiento de datos sea leal, de forma que el interesado, primero conozca que el tratamiento existe y además tenga información precisa sobre el mismo[626]. Para asegurar este objetivo, la Directiva 95/46/CE dispone de otras herramientas. Además del deber de informar, que se proyecta en este momento inicial del tratamiento de datos, la Directiva 95/46/CE dispone del mecanismo de publicidad del tratamiento (art. 21 Directiva 95/46/CE) y también del derecho de acceso que posibilitará que el interesado, en cualquier momento del tratamiento pueda conocer la información

---

aquellos conjuntos de datos que permiten conocer las características de la personalidad de una persona física (art. 18 y 21 Ley Liechtenstein).

[623] Así en la Ley italiana, para que el sector privado pueda tratar datos de este tipo se le exige, como regla general que se solicite el consentimiento por escrito del interesado y lo autorice la autoridad de control (art. 26 Ley italiana). En la Ley griega se exige para tratar este tipo de datos la autorización de la autoridad de control (art. 7.2 Ley griega). La Ley eslovena exige que este tipo de datos se etiqueten como sensibles y que se protejan por métodos criptográficos y firma electrónica cuando deban transmitires por redes de telecomunicaciones (art. 14, apartados 1 y 2 Ley eslovena).

[624] La Ley checa establece la posibilidad de que esta obligación de informar la pueda realizar el encargado en nombre del responsable (art. 11.7 Ley checa).

[625] Hay que recordar que el responsable del tratamiento, si no está establecido en el territorio de la UE y recurre a medios situados en el territorio de alguno de los Estados miembros para llevar a cabo tratamientos de datos personales debe nombrar a un representante en el territorio de este Estado miembro. Con esta obligación de informar al interesado se dota al representante de un papel que va más allá del de mero representante. No obstante, esto no implica que obligatoriamente el interesado deba dirigirse contra el representante, en caso de incumplimiento de esta concreta obligación o de las demás que sólo estén establecidas para el responsable del tratamiento, sino que puede ir también contra el responsable del tratamiento. Así lo establece el artículo 4.2 Directiva 95/46/CE al indicar "sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento". Ver Capítulo IV.

[626] En el Reino Unido se resalta esta conexión del deber de informar con el principio de lealtad y licitud, de forma que en la Parte II del Anexo 1 Ley inglesa, dedicada a la interpretación de este principio de lealtad y licitud es donde se desarolla la regulación del deber de informar. Por tanto, se especifica en esta disposición que para que se considere que los datos se tratan de forma leal deberá cumplirse con esta obligación de informar. De hecho, durante el proceso de elaboración de la Directiva 95/46/CE las delegaciones de Irlanda y Reino Unido, según indica HEREDERO HIGUERAS, mostraron dudas acerca de la necesidad de incluir en el texto de la Directiva 95/46/CE la regulación específica de la información al interesado, ya que entendían que lo que hacía era desarrollar el concepto de tratamiento leal para lo que bastaba con el artículo 6.1.a) Directiva 95/46/CE. M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, pág. 136.

sobre el mismo (art. 12 Directiva 95/46/CE). Se configura así un principio de transparencia que conjuga varios elementos para extenderse a todo el ciclo del tratamiento y que es requisito previo para asegurar el poder de control del interesado sobre sus datos.

Otra característica de este deber de informar es su carácter instrumental respecto al consentimiento, ya que permite cumplir con una de las características del mismo: que sea un consentimiento informado. En consecuencia, esta obligación sirve de complemento a uno de los supuestos de legitimación del tratamiento de datos. No obstante, eso no implica que se trate de un deber ligado exclusivamente a este supuesto de legitimación, sino que se erige como una obligación independiente, que se tendrá que cumplir también, cuando el tratamiento se realice en virtud del resto de supuestos habilitantes[627].

La Directiva 95/46/CE distingue en la regulación de este deber de informar dos posibles vías de obtención de los datos: la recogida de datos directa del propio interesado (art. 10 Directiva 95/46/CE) y la recogida de datos indirecta de otra fuente distinta del interesado (art. 11 Directiva 95/46/CE). En ambas vías se establece un contenido informativo obligatorio y otro contenido que es opcional[628]. Respecto a este segundo bloque de información optativa, los Estados miembros deben aplicar un test de necesidad, de forma que, si las circunstancias específicas que rodean la recogida de datos hacen

[627] La Ley húngara establece expresamente este carácter autónomo respecto al supuesto de legitimación consistente en la solicitud de consentimiento, ya que indica que la información debe proporcionarse al interesado de forma previa al inicio del tratamiento de sus datos e independientemente de que se precise o no el consentimiento (Sección 20 Ley húngara). Además de la obligación general de informar en algunas leyes nacionales se han regulado obligaciones específicas de información que suelen responder a las especiales características del entorno o el sector al que se aplican. Como ejemplos indicar los contenidos en los artículos 23 Ley islandesa y 21 Ley noruega que establecen obligaciones para informar en caso de elaboración de perfiles. Asimismo, en la Ley portuguesa se añade un supuesto de información que parece específico del contexto de Internet, de forma que establece que cuando los datos se recojan en redes abiertas (*open networks* o *redes abertas*) el interesado debe ser informado, excepto si ya ha sido previamente informado, de que sus datos personales pueden circular en la red sin medidas de seguridad y podrían ser accesibles y utilizados por terceros no autorizados (artículo 10.4 Ley portuguesa).

[628] En el caso en el que se obtienen los datos directamente del interesado, el bloque obligatorio incluirá: la identidad del responsable y, en su caso, de su representante y los fines del tratamiento de datos. En cuanto al bloque de información optativo se incluyen a modo de ejemplo los siguientes aspectos: los destinatarios o las categorías de destinatarios de los datos; el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder y, por último, la existencia de derechos de acceso y rectificación de los datos. Cuando los datos no se obtienen directamente del interesado, el bloque obligatorio es igual que en la recogida directa. En cambio en el bloque optativo, no se incluye como ejemplo de información adicional el carácter obligatorio o no de la respuesta y las consecuencias de la negativa a responder. Esta diferencia es lógica, ya que se parte de que los datos sobre los que se informa, ya se han incorporado en los sistemas del responsable y no cabe añadir contenido nuevo como podrían ser respuestas a cuestiones que se le pudieran plantear al interesado. Además se añade otro ejemplo de posible información adicional: las categorías de los datos. Así se pretende asegurar que el interesado tiene control sobre estos datos que él no ha entregado directamente.

preciso, para lograr un tratamiento de datos leal respecto al interesado, que se proporcione esta información adicional, ésta deberá comunicarse al mismo[629].

En ambos casos de recogida directa o indirecta de datos se establece una excepción que se refiere al hecho de que el interesado ya hubiera sido informado previamente de los extremos que se establecen por la regulación. Esta posibilidad tendrá especial sentido para la recogida indirecta, en la que debe entenderse que el origen de los mismos será otro responsable del tratamiento que podría haber informado antes de comunicar los datos[630].

Respecto a la comunicación, hay que indicar que, en caso de recogida indirecta, se establece el momento en el que deberá cumplirse con la obligación de informar, que se situará cuando se registran los datos, o si se tiene intención de comunicar los datos a un tercero, como máximo cuando se realice la primera comunicación[631].

También hay que tener en cuenta, en la recogida indirecta, que se establecen unas excepciones al deber de informar cuando el tratamiento tenga fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley[632].

---

[629] En la Ley Países Bajos, se establece con relación al bloque de información adicional, en los dos casos de recogida directa e indirecta de datos del interesado que será el responsable quien deberá decidir si es necesario proporcionarlo (art. 33.3 y 34.3 Ley Países Bajos).

[630] Sin embargo, como ejemplo de posibles interpretaciones divergentes, la Ley austríaca contempla como un tipo de recogida indirecta de datos cuando los datos provengan de una transmisión de otra aplicación de datos con diferente finalidad del mismo responsable o de una aplicación de datos de otro responsable (hay que tener en cuenta que la Ley austríaca utiliza el concepto "aplicación de datos" en la mayor parte del texto). Por tanto, se entiende, según esta ley, que aunque se transmitan los datos en el marco de la misma organización si se realizan estas transmisiones internas de una aplicación de datos a otra, al cambiar la finalidad a la que están destinadas, deberá cumplirse con este deber de información específico (parágrafo 24.3 Ley austríaca).

[631] El hecho de que se contemple esta obligación de informar antes de comunicar los datos parte de aceptar que se puedan comunicar los datos legítimamente a un tercero aunque ello no se hubiera previsto en el momento de recogida de datos (Considerando 39 Directiva 95/46/CE).

[632] Hay que recordar también las posibles limitaciones al derecho de información que permite el artículo 13 Directiva 95/46/CE. La Ley noruega establece, en este sentido, unas excepciones al derecho de información y derecho de acceso muy amplias. Entre las mismas hay que resaltar la que permite excepcionar estos derechos si no es aconsejable que el interesado conozca los datos, si una obligación de secreto profesional se aplica, si los datos están en documentos internos de trabajo o si fuera contrario a intereses privados o públicos fundamentales de proporcionar información, incluyendo el interés del interesado mismo (art. 23 Ley noruega).

Resulta evidente que el hecho de incluir un bloque de información optativa que debían elegir los Estados miembros ha dado lugar a diferencias entre las leyes[633]. La Comisión Europea resalta que, en algunas legislaciones, no se garantiza en absoluto el cumplimiento de este deber de informar[634]. Asimismo, la Comisión estima que deberían añadirse a este deber de informar otros aspectos, como los datos de contacto de la autoridad de control pertinente y la información relativa al tiempo de conservación de los datos[635].

3.4. La obligación de notificación a la autoridad de control

3.4.1. La obligación de notificación

La Directiva 95/46/CE establece la obligación de notificación a la autoridad de control de las características del tratamiento, de forma previa a realizarlo (art. 18

[633] A modo de ejemplo, en la Ley italiana se establece que el interesado tiene derecho a que se le informe sobre la identidad del responsable, de los encargados del tratamiento y de las entidades o categorías de entidades a quienes se les comunique los datos o la persona autorizada a realizar el tratamiento. Además se especifica que, en caso de que hayan varios encargados del tratamiento se permite que se de la información de uno de ellos y que en la web corporativa se proporcione la información del resto de encargados. Esta información correspondería a la relativa a los destinatarios que especifica la Directiva 95/46/CE (art. 13 Ley italiana). En Francia se incluyen todos los puntos, los de ambos bloques y además se añade la información sobre las transferencias a países no miembros de la UE. Sin embargo, cuando los datos se recojan mediante cuestionarios, la Ley francesa sólo obliga a informar de la identidad del responsable y, en su caso, de su representante, la finalidad del tratamiento, el carácter obligatorio o facultativo de las respuestas y la posibilidad de ejercer los derechos que se otorgan a los interesados (art. 32 Ley francesa). También hay que resaltar que en la Ley francesa esta obligación se encuentra en el apartado que este texto dedica expresamente a las obligaciones de los responsables del tratamiento.

[634] *Commission Staff Working Paper, Impact assessment accompanying the document Regulation of the European Parliament […], op. cit., Annex 2,* págs. 30 a 31. Por otro lado, el hecho de que la ley inglesa en la regulación de este deber de información prevea que "el responsable debe asegurar, si fuera factible (*practicable* en la versión original), que el interesado tiene, recibe o se le ha proporcionado, la siguiente información: […]" tanto en el supuesto de recogida directa como indirecta de datos del interesado, no puede considerarse que respete la regulación de la directiva que no admite esta previsión que dejaría al arbitrio del responsable el hecho de valorar si es factible o no el hecho de cumplir con la obligación de informar. Así lo entiende también D. KORFF, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Contract _r: JLS/2008/C4/011 – 30-CE-0219363/00-28, Country Studies, A.6-United Kingdom, op. cit*., pág. 40-41. Tampoco entiendo que se cumpla con el deber de informar, cuando la autoridad de control inglesa (ICO) indica que en lo que se refiere a los fines del tratamiento, no debe informarse de lo obvio, *Privacy notices code of practice*, *Information Commissioner's Office* (ICO), p 12, http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_notices_cop_final.pdf, (fecha de consulta: 24.8.13). Por último respecto a la Ley inglesa, en el contenido de la información que debe proporcionarse directamente al interesado, no incluye los ejemplos que da la Directiva entre los que figuran "los destinatarios o las categorías de destinatarios de los datos". Por tanto, en el marco de esta ley, nada impide que se puedan comunicar los datos sin informar al interesado, siempre que se cumpla con los otros principios establecidos por la ley.

[635] *Commission Staff Working Paper, Impact assessment accompanying the document Regulation of the European Parliament […], op. cit., Annex 2,* pág. 32.

Directiva 95/46/CE). El objetivo que se persigue con esta obligación es la publicidad de los tratamientos y el control de los mismos (Considerando 48 Directiva 95/46/CE). El cumplimiento de esta obligación de notificación se asigna expresamente al responsable del tratamiento o a su representante (art. 18.1 Directiva 95/46/CE). Sin embargo, algunas leyes nacionales también permiten que el encargado del tratamiento realice esta notificación[636].

La publicidad se consigue mediante la llevanza por parte de las autoridades de control de un registro de los tratamientos notificados (art. 21 Directiva 95/46/CE). De esta forma, se facilitará el ejercicio de los derechos, como el de acceso, por parte de los interesados[637]. En algunas leyes nacionales se ha estipulado un derecho por parte de las personas a la consulta de este registro[638].

La Directiva 95/46/CE permite que los Estados miembros determinen el contenido de la información a notificar pero incluye un contenido mínimo que deben respetar[639] y además establece la necesidad de que se prevean procedimientos para modificar esta información (art. 19 Directiva 95/46/CE)[640]. Entre la información que han añadido las legislaciones nacionales se puede citar la relativa a las personas que se ocupan del

[636] Artículo 16.1 Ley irlandesa, artículo 53 Ley danesa y artículo 36.3 Ley finlandesa. La Ley letona establece la obligación de notificar los tratamientos de datos que se quieren llevar a cabo, pero no indica que el obligado deba ser el responsable, sino que alude a las instituciones del gobierno local o estatal, las personas físicas o jurídicas (art. 21.1 Ley letona).

[637] El Considerando 13 de la Propuesta de Directiva de 1990 indicaba que el procedimiento de notificación perseguía asegurar la transparencia indispensable para el ejercicio del derecho de acceso del interesado a los datos que le conciernen. M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, pág. 165.

[638] Artículo 29 Ley eslovena, artículo 14 LOPD.

[639] El contenido mínimo será el siguiente: el nombre y la dirección del responsable del tratamiento y, en su caso, de su representante; el o los objetivos del tratamiento; una descripción de la categoría o categorías de interesados y de los datos o categorías de datos a los que se refiere el tratamiento; los destinatarios o categorías de destinatarios a los que se pueden comunicar los datos; las transferencias de datos previstas a países terceros; una descripción general que permita evaluar de modo preliminar si las medidas adoptadas en aplicación del artículo 17 Directiva 95/46/CE referido a la seguridad del tratamiento, resultan adecuadas para garantizar esta seguridad (art. 19 Directiva 95/46/CE).

[640] Incluso se establece la modificación que de oficio puede llevar a cabo la autoridad de control si conociera que ha habido algún cambio. En este sentido la Ley austríaca establece que la Comisión de Protección de Datos, autoridad de control de Austria, podrá de oficio modificar la información registrada si conoce mediante las publicaciones oficiales que hay algún cambio en los datos del responsable, si la base jurídica utilizada por el responsable para legitimar el tratamiento ya no es válida, si se tuviera que suprimir la aplicación de datos al haber expirado el límite temporal establecido en el procedimiento de registro o si no se tratan datos (parágrafo 22.1 y 2 Ley austríaca). Establecen la obligación de notificar los cambios en la información notificada: la Sección 20 Ley inglesa, el artículo 13.2 Ley luxemburguesa, el artículo 27.2 Ley eslovena, el artículo 22.4 Ley letona, el artículo 32 Ley islandesa, el artículo 19 Ley checa y también lo establece la legislación española (arts. 26.3 LOPD y 58 RLOPD).

tratamiento de los datos[641], la que responde a aspectos específicos de la regulación[642], así como la que responde a aspectos relativos al tratamiento como la duración o la base habilitante del mismo[643]. Por último, indicar que en algunos Estados miembros se ha establecido para este trámite de notificación el pago de una tasa[644].

Parece deducirse de la regulación contenida en la Directiva 95/46/CE que la notificación es una obligación meramente formal, sin que la entidad registradora -la autoridad de control- lleve a cabo un examen de este contenido, con el fin de detectar si es lícito el tratamiento[645]. Sin embargo, en algunas legislaciones nacionales se ha establecido una revisión más exigente de la notificación, que puede llevar incluso a denegar la misma si la autoridad entiende que puede existir incumplimiento de la normativa[646].

[641] Artículo 4e Ley alemana, artículo 30 Ley francesa, artículo 29 Ley portuguesa, artículo 22.1) Ley letona, artículo 32 Ley islandesa, artículo 15.g Ley de Liechtenstein, artículo 32 Ley noruega. La LOPD establece la obligación de notificar al encargado de tratamiento.

[642] La Ley austríaca incluye los datos relativos al operador en caso de que la aplicación de datos notificada se refiera a un "sistema conjunto de información" (parágrafo 19 Ley austríaca). La Ley francesa añade como información que debe notificarse: las interconexiones y cualquier forma de relacionar los tratamientos (art. 30 Ley francesa). La Ley portuguesa añade las interconexiones de datos (art. 29 Ley portuguesa).

[643] Así, por ejemplo, la Ley francesa añade como información que debe notificarse el origen de los datos personales tratados, la duración de la conservación de los datos (art. 30 Ley francesa). La Ley austríaca incluye la evidencia de la competencia o autoridad que permite la actividad del responsable, si se requiere (parágrafo 19 Ley austríaca). La Ley griega incluye la obligación de notificar la dirección donde el fichero o la mayor parte del *hardware* que da soporte al tratamiento de datos está establecido (art. 6.2.b Ley griega). La Ley danesa contempla la obligación de notificar la fecha de inicio del tratamiento y la de borrado de los datos (43.2.8 y 9 Ley danesa). La Ley luxemburguesa añade el supuesto de legitimación del tratamiento de datos (art. 13.1.b Ley luxemburguesa).

[644] Se ha establecido el pago de una tasa en la Sección 18 Ley inglesa, artículo 17.2 Ley irlandesa, artículo 63.1 Ley danesa, artículo 13.2 Ley luxemburguesa y Sección 67 Ley húngara.

[645] Así parece extraerse por contraste con el artículo 20 Directiva 95/46/CE que sí prevé un control previo para ciertos tratamientos y del Considerando 52 Directiva 95/46/CE que estima suficiente el control *a posteriori* por parte de las autoridades competentes. En este sentido la Ley húngara establece que si se proporciona toda la información obligatoria se registrará el tratamiento y se proporcionará al responsable un número de registro que se asigna a efectos de identificar el tratamiento de datos y no implica la verificación de la legitimidad de éste (Sección 68 Ley húngara). En la Ley francesa se deja claro que la notificación (a la que se refiere como declaración, "*déclaration*") comporta el compromiso por parte del declarante de que el tratamiento sobre el que realiza esta notificación cumple con lo establecido en la ley (art. 23.I Ley francesa).

[646] Así, por ejemplo, en la Ley irlandesa la autoridad de control realiza un examen de la solicitud y puede denegar la inscripción si considera que los datos son insuficientes o no se proporciona la información que decida solicitar o es aparente que la persona solicitante incumplirá alguna de las disposiciones de la ley (art. 17 ley irlandesa). Además en esta ley se limita la duración de las inscripciones que normalmente será de un año, a no ser que el registro sea continuado. El responsable no puede mantener los datos personales a no ser que esté vigente la inscripción y mientras debe ajustarse a la información notificada. Lo mismo sucede respecto al encargado del tratamiento que no podrá tratar los datos a no ser que esté inscrito en el registro. Los empleados o agentes del responsable estarán sujetos a las mismas restricciones de uso y manejo de los datos de forma que deben ajustarse a la información que consta registrada (arts. 16 a 20 Ley irlandesa).

Por otro lado, la Directiva 95/46/CE establece que los Estados miembros deberán precisar aquellos tratamientos, que puedan suponer riesgos específicos para los derechos y libertades de los interesados, respecto a los que se especifica que se realizará un examen previo a su puesta en marcha, por parte de la autoridad de control, o del encargado de protección de datos (art. 20 Directiva 95/46/CE). Esta comprobación también podrá realizarse durante el proceso de la elaboración de una norma[647]. Si se acude a las legislaciones nacionales para ver qué tratamientos han considerado susceptibles de tener que someterse a este control previo, se observa que en su mayoría responden a tratamientos en los que están implicadas las categorías especiales de datos o que se incardinan en sectores problemáticos, como los de crédito y solvencia[648]. En otros casos se ha establecido que se desarrolle posteriormente, lo que parece más acertado porque así se pueden tener en cuenta los riesgos emergentes[649].

En un principio la obligación de notificación sólo se refiere a un tratamiento o un conjunto de tratamientos que podrán ser total o parcialmente automatizados, dejando fuera a los no automatizados[650]. No obstante, se deja al arbitrio de los Estados miembros

[647] En este sentido, el Considerando 54 Directiva 95/46/CE indica que el examen previo puede realizarse "en el curso de la elaboración de una medida legislativa aprobada por el Parlamento nacional o de una medida basada en dicha medida legislativa, que defina la naturaleza del tratamiento y precise las garantías adecuadas".

[648] Así por ejemplo la Ley alemana incluye esta obligación de llevar a cabo un control previo para tratamientos que presenten riesgos específicos para los derechos de los afectados, entre los que incluye los relativos a categorías especiales de datos y los que pretendan el conocimiento de la personalidad del interesado, incluyendo sus habilidades, rendimiento o conducta (arts. 4d.5 y 6 Ley alemana). En la Ley francesa se establece una amplia regulación sobre los tratamientos sometidos a este control previo entre los que figuran los destinados a fines estadísticos, los relativos a categorías especiales de datos anonimizados o cuyo uso se justifica por el interés público, a datos genéticos (con excepciones), los tratamientos que tienen por finalidad interconectar ficheros entre varios responsables y con fines diferentes, los que incluyen el número de identificación nacional de las personas; los que se refieren a asuntos sociales y a datos biométricos (arts. 25 a 29 Ley francesa). La Ley portuguesa considera que deben someterse a control previo los tratamientos relativos a categorías especiales de datos, los relativos al crédito y la solvencia de los interesados, las interconexiones de datos y el uso de datos para fines que no dan lugar a su recogida. (art. 28 Ley portuguesa). Otros ejemplos se pueden encontrar en los artículos 45.1 y 50.1 Ley danesa, en el artículo 24 Ley Países Bajos, en el artículo 24 Ley lituana, en el artículo 14 Ley luxemburguesa, en el artículo 17b Ley búlgara y en el artículo 33 Ley noruega.

[649] Entre las leyes que establecen este desarrollo posterior están la Sección 41 Ley sueca, artículo 34 Ley maltesa, Sección 22 Ley inglesa, artículo 31.3 Ley danesa, artículo 22.2 Ley letona, artículo 23 Ley rumana y artículo 12A Ley irlandesa.

[650] Así se ha estipulado en la Ley francesa (art. 22), la Ley irlandesa (art. 16.1.a.ii), Ley lituana (art. 31.1). En la Ley Países Bajos los tratamientos no automatizados sólo deberán notificarse si son objeto de control previo (art. 27.2 Ley Países Bajos). Según la Ley maltesa sólo deben notificarse, de forma previa a su inicio los tratamientos total o parcialmente automatizados, por lo que no sería obligado notificar los ficheros manuales (art. 29.1 Ley maltesa). En la Ley islandesa se obliga a notificar los tratamientos en los que se utilice tecnología electrónica (art. 31 Ley islandesa). La Ley noruega obliga a notificar los tratamientos de datos por medios automatizados y los tratamientos manuales de datos sensibles (art. 31 Ley noruega).

el que puedan disponer la notificación de algunos o todos los tratamientos no automatizados eventualmente de forma simplificada[651].

Además del supuesto indicado de simplificación para los ficheros manuales, se permite a los Estados miembros que puedan disponer la simplificación o la omisión del deber de notificación en otros supuestos. Estos supuestos son, en primer lugar, cuando los tratamientos no puedan afectar a los derechos y libertades de los interesados, habida cuenta de los datos a que se refiere el tratamiento (art. 18.2 Directiva 95/46/CE)[652].

Un segundo supuesto es cuando sean tratamientos que lleven a cabo las fundaciones o cualquier otro organismo sin ánimo de lucro con una finalidad política, filosófica, religiosa o sindical, en el curso de sus actividades legítimas y con las debidas garantías, siempre que se refieran a sus miembros o a las personas que mantengan contactos regulares con esta entidad por razón de su finalidad (art. 18.4 Directiva 95/46/CE)[653]. Finalmente, los Estados podrán optar por esta simplificación u omisión, cuando los tratamientos los lleven a cabo registros públicos (art. 18.3 Directiva

[651] La Ley austríaca dispone que sólo los ficheros manuales que se refieran a datos sensibles, actos criminales o información sobre crédito deberán notificarse al registro (parágrafo 17.1 Ley austríaca). En la Ley portuguesa sólo se obliga a notificar los tratamientos no automatizados que incluyan datos de categorías especiales y que tengan como fin la protección del interés vital del interesado o de otra persona cuando el interesado no sea capaz de otorgar su consentimiento (art. 27.5 Ley portuguesa). El resto de tratamientos no automatizados, por lo tanto, no debe notificarse. No obstante, hay que precisar que en el Vademecum realizado por el GA29 sobre el trámite de notificación a las autoridades de control en los diferentes países miembros se especifica en el cuestionario que respondió la autoridad de control portuguesa que sí es obligatorio notificar los tratamientos no automatizados, *Vademecum on notification requirements, version as of 3.7.2006, pursuant to the Working Party document Nº WP106, Article 29 Data Protection Working Party*, pág. 58. La legislación española obliga a la notificación de ficheros automatizados o no automatizados indistintamente.

[652] La dificultad radica en la determinación de estos tratamientos. Respecto a la determinación de estos tratamientos por las leyes nacionales se puede hacer referencia a algunos de los supuestos más habituales que se incluyen: los tratamientos de datos accesibles al público (art. 18.1 Ley checa, parágrafo 17.2 Ley austríaca, art. 21.2 Ley letona, art. 7.6 Ley chipriota y art. 31 Ley islandesa); tratamientos de datos impuestos por ley (art. 18.1 Ley checa, art. 36.4 Ley finlandesa, art. 7a Ley griega y art. 7.6 Ley chipriota), tratamientos realizados para llevar a cabo gestiones ordinarias de los responsables (art. 36.4 Ley finlandesa, art. 7a Ley griega, parágrafo 17.2 Ley austríaca, art. 49.1 Ley danesa, art. 2.15 Ley lituana, art. 12.2 y 3 Ley luxemburguesa, Sección 65 Ley húngara y art. 7.6 ley chipriota) y tratamientos que realicen responsables de reducidas dimensiones (art. 7.4 en relación con art. 26 y 27 Ley eslovena, art. 4d Ley alemana). En algunos casos la ley lo que prevé es un posterior desarrollo de estos supuestos (art. 29 Ley Países Bajos, art. 17 Ley croata, Sección 23 Ley inglesa, art. 44.4 y 49.3 Ley danesa, art. 15.6 Ley Liechtenstein, art. 31 Ley noruega, art. 17a Ley búlgara, art. 37 Ley italiana, art. 22.9 Ley rumana, art. 24 Ley francesa y ar. 31 Ley islandesa).

[653] A modo de ejemplo se pueden citar algunas disposiciones que incluyen esta exención: artículo 16.1.b Ley irlandesa, artículo 18.1 Ley checa, artículo12.3.f) Ley luxemburguesa, artículo 7a Ley griega.

95/46/CE)[654] y cuando el responsable del tratamiento designe un encargado de protección de los datos personales (art. 18.2 Directiva 95/46/CE), en los términos que se indicarán más adelante.

En caso de que el responsable se beneficie de alguno de estos supuestos de simplificación o de exención de la obligación de notificación, ello no le dispensa del cumplimento del resto de obligaciones establecidas en la directiva (Considerando 51 Directiva 95/46/CE).

Este trámite de notificación ha sido criticado por entender que aporta una excesiva burocracia. Las amplias opciones que brindaba la propia Directiva 95/46/CE de flexibilidad han originado que los responsables que se ubican en varios Estados miembros deban cumplir con un trámite que en cada Estado es diferente[655].

3.4.2. El encargado de protección de datos personales

La inclusión de esta figura respondió a una demanda de la delegación germana durante el proceso de elaboración en la Directiva 95/46/CE, ya que ésta se contenía en la Ley federal alemana de 1990[656]. Al establecerse como una posibilidad para los Estados miembros, que quisieran adoptar la opción de exención o simplificación de notificación, sólo algunos de estos la han contemplado en su legislación nacional[657]. No obstante,

[654] Como ejemplo citar el artículo 16.1.a.i Ley irlandesa o el artículo 21.2 Ley letona que establecen esta exención.

[655] *Commission Staff Working Paper, Impact assessment accompanying the document Regulation of the European Parliament […], op. cit., Annex 2*, pág. 35.

[656] M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, pág. 170.

[657] Estos Estados son: Alemania (arts. 4d, 4f y 4g Ley alemana), Países Bajos (art. 62 Ley Países Bajos), Hungría (Secciones 24 y 25 Ley húngara), Francia (art. 22 Ley francesa), Reino Unido (Sección 23 Ley inglesa), Suecia (Secciones 37 a 40 Ley suecia), Estonia (art. 30 Ley estonia), Eslovaquia (art. 23 ss. Ley eslovaca), Letonia (art. 21 Ley letona), Lituania (art. 32 Ley lituana), Luxemburgo (arts. 12.2.a y 40 Ley luxemburguesa), Malta (art. 30 ss. Ley maltesa) e Islandia (art. 35 Ley islandesa). No se ha incluido, por tanto, en la legislación española. El *Beauftragter für den Datenschutz* o *Data Protection Official*, como se le denomina en la Ley alemana, es de designación obligatoria, excepto en el caso de que el tratamiento no sea automatizado y lo lleven a cabo menos de 20 personas. Tampoco es obligatorio para organizaciones del sector privado que no destinen como máximo 9 empleados al tratamiento de datos. También se establecen ciertas activivades del sector privado, como el marketing, en las que deberá realizarse la designación independientemente de las personas que se dediquen al tratamiento (art. 4f Ley alemana). La Ley húngara establece la obligatoriedad de su designación para ciertos colectivos (Secciones 24 y 25 Ley húngara) y la Ley islandesa deja en manos de la autoridad de control que pueda obligar a un responsable a hacer esta designación (art. 35 Ley islandesa). Otras leyes dejan la opción de realizar la designación en manos del responsable, de forma que si así lo hacen podrán acogerse a la exención o simplificación de la obligación de

como señala la Comisión Europea, esta figura ha sido incorporada en organizaciones multinacionales y del sector público de forma natural, con el fin de poder hacer frente al cumplimiento de la normativa de protección de datos[658].

La Directiva 95/46/CE no contempla una definición del encargado de protección de datos personales y, por tanto, no contamos con elementos definitorios del mismo[659]. Lo único que se especifica es que podrá ser un empleado del responsable o un sujeto externo (Considerando 49 Directiva 95/46/CE)[660] y que debe gozar de independencia en el ejercicio de sus funciones (art. 18.2 y Considerando 49 Directiva 95/46/CE)[661]. Las leyes nacionales en algunos casos han establecido algunos requisitos que debería cumplir este sujeto. Especialmente estas características tienen que ver con su perfil profesional, ya que debe tener la capacidad necesaria para desempeñar las funciones que se le atribuyen[662].

---

notificación. Ejemplo de estas regulaciones son el artículo 12.2.a Ley luxemburguesa, artículo 22 Ley francesa, artículo 27 Ley estonia, artículo 21.2 Ley letona y artículo 30.2 Ley maltesa.

658 *Commission Staff Working Paper, Impact assessment accompanying the document Regulation of the European Parliament […], op. cit., Annex 2,* pág. 35.

659 Entiende SANTAMARÍA RAMOS que se trata de un encargado del tratamiento independiente. Si bien es cierto que puede encajar en la definición de encargado del tratamiento del artículo 2.e) de la Directiva 95/46/CE si se abstrae del resto de la regulación, no creo que fuera la intención del legislador incluirlo en esta definición. F.J. SANTAMARÍA RAMOS, *El encargado independiente. Figura clave para un nuevo derecho de protección de datos, op. cit.*, pág. 95.

660 El Considerando 49 Directiva 95/46/CE establece "que la persona encargada de la protección de los datos, sea o no empleado del responsable del tratamiento de datos, deberá ejercer sus funciones con total independencia;".

661 Las leyes nacionales también han recogido esta característica y así la ley alemana dispone que reportarán directamente al jefe de la entidad pública o privada. Deben contar con libertad e inmunidad, de forma que no les pueda penalizar por la ejecución de sus tareas y además la ley regula cómo puede ponerse fin al cargo (art. 4.g Ley alemana). La Ley luxemburguesa también dispone que goza de independencia con relación al responsable del tratamiento, debe disponer del tiempo pertinente y las actividades que ejerza paralelamente no deben generarle conflictos de interés con su misión. No puede ser objeto de represalias por parte de su empleador por el ejercicio de su misión, excepto si incumple obligaciones legales o convencionales (art. 40 Ley luxemburguesa). La Ley francesa establece la imposibilidad de que le sancione el empleador por razón de sus tareas (art. 22 Ley francesa). La Ley estonia regula que esta persona debe ser independiente en sus actividades respecto al responsable y monitorizar el cumplimiento de lo establecido en la legislación de protección de datos. Si esta persona ha informado al responsable de alguna vulneración y éste no adopta medidas para finalizarla deberá informar inmediatamente a la autoridad de control (art. 30 Ley estonia). La Ley húngara dispone que debe reportar directamente al jefe de la organización (Secciones 24 y 25 Ley húngara). La Ley Países Bajos establece que no podrán recibir instrucciones del responsable o la organización que lo haya designado y no podrán sufrir ninguna desventaja como consecuencia de desarrollar sus funciones (art. 63.2 Ley Países Bajos).

662 Así, la Ley alemana exige que sean personas con unos conocimientos especializados y una responsabilidad adecuada a sus tareas. Se permite que esta persona sea externa a la entidad (art. 4.f Ley alemana). La Ley luxemburguesa exige que sean personas físicas o jurídicas que debe admitir la autoridad de control, admisión que está subordinada a la justificación de una formación universitaria en derecho, economía, gestión de empresas, ciencias de la naturaleza o informática o que desempeñen las profesiones reguladas siguientes: abogados, supervisores de empresas, expertos contables y médicos. Además se establece que la autoridad de control realizará un control continuo de las cualidades del encargado y se puede oponer en todo momento a la designación o al mantenimiento de éste si no presenta las cualidades requeridas o si tiene de antemano una relación con el responsable del tratamiento de forma que hace que

En la Directiva 95/46/CE se definen las obligaciones que deberá llevar a cabo, con el fin de que pueda establecerse la exención o simplificación de notificación: tendrá que asegurarse que, en el ámbito interno del responsable, se cumpla con lo que establezca la normativa nacional adoptada, en virtud de la directiva, y debe llevar un registro de los tratamientos efectuados por el responsable. Las leyes nacionales además de establecer estas obligaciones, también disponen en algunos casos una obligación de secreto que deben cumplir estos encargados[663], la necesaria consulta a la autoridad de control[664], así como otras obligaciones adicionales[665]. Con el fin de que pueda desempeñar sus funciones también se le atribuyen en algunos casos facultades[666].

4. OBLIGACIONES DE CARÁCTER TRANSVERSAL RESPECTO AL CICLO DEL TRATAMIENTO

4.1. El respeto a los principios relativos a la calidad de los datos

Si bien los principios relativos a la calidad de los datos tienen un carácter transversal respecto al ciclo del tratamiento de datos, algunos hacen referencia a la fase de

surja un conflicto de intereses (art. 40 Ley luxemburguesa). La Ley francesa también exige que sea una persona con conocimientos específicos para poder realizar sus tareas (art. 22 Ley francesa) y, en esta misma línea la Ley Países Bajos exige que sean personas físicas que posean conocimientos adecuados para llevar a cabo sus funciones y que puedan ser considerados dignos de confianza (art. 63.1 Ley Países Bajos). La Ley húngara exige que tenga una licenciatura de derecho, económicas, tecnologías de la información o un equivalente (Secciones 24 y 25 Ley húngara) y la Ley letona que sea una persona física con un alto nivel de formación en jurisprudencia, tecnologías de la información o similar (art. 21.1.2 Ley letona).

[663] La Ley alemana dispone que este encargado está obligado a mantener secreto sobre la identidad de los interesados y las circunstancias que permitan a los interesados que sean identificados, a no ser que el interesado le libere. También establecen esta sumisión a una obligación de secreto: artículo 24 Ley luxemburguesa, artículo 63.4 Ley Países Bajos y artículo 21.2.3 Ley letona.

[664] Artículo 4g Ley alemana, artículo 40.5 Ley luxemburguesa, el artículo 64.4 Ley Países Bajos, el artículo 30 Ley estonia.

[665] Incluyen otras obligaciones diferentes: Secciones 24 y 25 Ley húngara, artículos 63.5 y 64.1 y 2 Ley Países Bajos, artículo 21.2.4 Ley letona, artículo 32.2 Ley lituana, artículo 31 Ley maltesa.

[666] La Ley alemana, respecto al deber de secreto que tenía el encargado, también lo contempla como un derecho ya que cuando, en el marco de sus actividades, el encargado conozca datos por los que el jefe de una entidad del sector público o privada o una persona empleada por esta entidad tenga derecho a negarse a dar evidencias, este derecho también se le aplicará al encargado y a sus asistentes (art. 4f Ley alemana). La Ley luxemburguesa dispone que tendrá poder de investigación, con el fin de asegurar el cumplimiento de la ley por el responsable del tratamiento y derecho de obtener información y de informar al responsable de las formalidades que debe éste cumplir (40.2 Ley luxemburguesa). En la Ley francesa la consulta a la autoridad de control para obtener ayuda sobre sus funciones, es una opción para el encargado (art. 22 Ley francesa). La Ley letona dispone que el responsable le tiene que proporcionar las herramientas necesarias y el tiempo necesario dentro del horario laboral para desarrollar sus funciones (art. 21.1.3 Ley letona). También lo dispone la Ley lituana según la que el responsable está obligado a proporcionar a esta persona información completa sobre el tratamiento de datos programado y la intención de utilizar medios automatizados para que de su opinión (art. 32.3 Ley lituana).

recogida. Resulta imprescindible que el responsable analice, de forma previa a esta recogida, los datos que requiere para los fines que persigue con el tratamiento. Hay que recordar que los fines y los medios del tratamiento son los aspectos sobre los que se proyecta la capacidad de decisión del responsable.

La Directiva 95/46/CE establece que el cumplimiento de estos principios corresponde a los responsables del tratamiento (art. 6.2 Directiva 95/46/CE). Esta previsión suscita alguna duda, ya que, si en los otros artículos no se especifica lo mismo, ¿significa que no deberá cumplirlos el responsable?, ¿entonces quién? Puede entenderse que lo que quiere decir es que, pese a que sea el responsable quien debe garantizar su cumplimiento, podrá encomendarlo a otros sujetos, como el encargado del tratamiento.

La transposición de estos principios de calidad a la legislación nacional se ha realizado en términos similares a la Directiva 95/46/CE, si bien el GA29 ha señalado que ha habido interpretaciones divergentes de los mismos[667]. También lo ha indicado la Comisión Europea que atribuye las diferencias de interpretación a la indeterminación de los términos que conforman estos principios[668].

4.1.1. Principios de lealtad y licitud

Los responsables deben tratar los datos de manera leal y lícita (art. 6.1.a) Directiva 95/46/CE). Pero ¿qué significa exactamente tratar los datos de manera leal y lícita? Por tratamiento leal hay que entender aquel que el responsable realiza desde la honestidad, desde la buena fe, en el marco de su relación con el interesado. Así lo apunta la Directiva 95/46/CE, cuando entiende que un tratamiento leal de datos exige que el interesado conozca la existencia de ese tratamiento y cuente con la información precisa y completa exigible de acuerdo con su derecho de información establecido en la directiva. Se orienta, por lo tanto, a la transparencia que debe regir el tratamiento, como máxima garantía que permitirá al interesado tener la capacidad de controlar el tratamiento[669]. Para poder actuar,

[667] De esta forma, se aplican criterios diversos para la determinación de lo que se considera tratamiento incompatible con los fines para los que se recogieron los datos o lo que se consideran fines explícitos. *Opinion 3/2013 on purpose limitation, 00569/13/EN WP 203, 2.4.2013, Article 29 Working Party*, pág.10.

[668] *Commission Staff Working Paper, Impact assessment accompanying the document Regulation of the European Parliament […], op. cit., Annex 2*, págs. 25 a 26.

[669] El GA29 en su análisis del principio de finalidad indica que este principio, en concreto, contribuye a la transparencia, la seguridad jurídica, el poder predecir el uso de los datos. Además, de esta forma se

el individuo, primero, precisa conocer que el tratamiento se lleva a cabo y las circunstancias que rodean al mismo.

Entiendo que la lealtad también se extiende a todos los principios establecidos en la Directiva 95/46/CE, así como sucede con la legitimidad. De esta forma, lealtad y licitud se mezclan para dar paso a la regulación que se incluye en esta norma. La lealtad es el espíritu de lo que se contiene en la normativa, como criterio que debería regir la actuación del responsable frente al interesado y que se traduce en la regulación de obligaciones y derechos existente. Por eso, hay términos que se encuentran en esta norma que muestran esta inspiración, como el interés legítimo.

Un tratamiento de datos lícito supone que respeta la legislación que gobierne el tratamiento de datos. Esta legislación será principalmente la que transponga la Directiva 95/46/CE, pero también otra normativa que pueda aplicarse a este tratamiento de datos, en función del sector en el que esté encuadrado el mismo[670]. Algunas legislaciones nacionales consideran que el responsable debe respetar las buenas prácticas o un especial deber de cuidado[671]. Este concepto de buenas prácticas conjugaría aspectos de lealtad y licitud, ya que, por un lado, equivaldría a incentivar el correcto desempeño del responsable en la gestión de los datos personales y, por el otro, le llevaría a respetar tanto las leyes, normas, como los usos y costumbres que, en el sector, existieran al respecto del tratamiento de los datos.

---

establecen límites en el modo en que los responsables utilizan los datos pero también se proporciona cierta flexibilidad a estos, por ejemplo con la noción de compatibilidad de los fines del tratamiento. *Ibídem*, pág. 11.

[670] La autoridad de control inglesa se refiere al término "licitud", de forma que entiende que califica a un tratamiento de datos que no pueda significar la comisión de una infracción penal, una violación de una obligación de confianza, una actuación que excede de la competencia legal atribuida o de un ejercicio incorrecto de esta competencia, una infracción del *copyright*, una violación de una obligación contractual, una violación de legislación o regulaciones sectoriales, una violación de la ley de derechos humanos (*Human Rights Act 1998*) que incorpora la Convención Europea de Derechos Humanos. *The guide to data protection, op. cit*, pág. 51.

[671] En la Ley maltesa y referido al principio de calidad se especifica como única diferencia respecto a la Directiva 95/46/CE que los datos deberán tratarse de acuerdo con las buenas prácticas (art. 7.b Ley maltesa). La Ley finlandesa erige como uno de sus principios el deber de cuidado de los datos (art. 5 Ley finlandesa).

4.1.2. Principio de finalidad

El principio de finalidad establece que los datos personales sean "recogidos con fines determinados, explícitos y legítimos y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas" (art. 6.1.b) Directiva 95/46/CE).

Si bien esta obligación también debe configurarse como transversal al ciclo lógico del tratamiento de datos, tiene especial incidencia en el momento de la recogida y, en lo que se conoce, como tratamiento ulterior de los datos. Este tratamiento ulterior de los datos describe aquel tratamiento que surge cuando los datos están ya incorporados al sistema de información del responsable, como elaboraciones de estos datos *a posteriori*[672].

En el análisis previo que deberá realizar el responsable, antes de la recogida de datos, debería incluir, como uno de los aspectos clave a estudiar, el de la finalidad del tratamiento[673]. Los datos deberán utilizarse para fines determinados, explícitos y legítimos. El GA29 describe estos tres requisitos y considera que, el hecho de que los fines sean determinados, exigiría que estén suficientemente definidos para asegurar que se cumple con todas las medidas de protección adecuadas y, de forma, que se delimite el ámbito del tratamiento. El requisito de que los fines sean explícitos implicaría que no deberían ser ambiguos ni ocultos. Por último, que los fines sean legítimos iría más allá de lo que se considera como fundamento para habilitar el tratamiento, que debe hallarse en el artículo 7 Directiva 95/46/CE, y se referiría al respeto de otras legislaciones[674].

En concreto, la determinación de estos fines debe realizarse, como muy tarde, en el momento de obtener los datos[675]. Si hay varios fines deberán aplicarse todos los requisitos que exige el artículo 6 Directiva 95/46/CE para cada uno de ellos por separado,

[672] El GA29 define el tratamiento ulterior de datos como toda operación de tratamiento de datos que sea posterior a la primera operación que exige todo tratamiento: la recogida de datos. *Opinion 3/2013 on purpose limitation, op. cit.*, pág. 21.
[673] Como indica el GA29 la finalidad del tratamiento es la "*raison d'être*" del tratamiento. *Opinion 3/2013 on purpose limitation, op. cit.*, pág. 11.
[674] Para un estudio en detalle de estos tres requisitos ver *Ibídem*, págs. 17 a 20.
[675] Así lo concreta el Considerando 28 de la Directiva 95/46/CE y *Ibídem*, pág. 15.

de forma que cada uno de estos fines debe ser determinado individualmente y, por ejemplo, no todos los datos que puedan recogerse al mismo tiempo, para varios fines, tendrán que ser necesarios para todos ellos[676].

La Carta UE, en su configuración del derecho a la protección de datos, hace referencia a los principios de calidad relativos a la lealtad en el tratamiento de datos y a la concreción de la finalidad y también alude a la necesaria legitimación del tratamiento (art. 8.2 Carta UE). La legitimación del tratamiento que se está regulada en el artículo 7 Directiva 95/46/CE y el cumplimiento de los principios de calidad del artículo 6 Directiva 95/46/CE deben considerarse requisitos acumulativos que deberá cumplir el responsable del tratamiento[677].

Este aspecto acumulativo de ambos principios, calidad y legitimación, tiene su trascendencia, ya que implica que el responsable que recoge los datos para un fin determinado, después no puede tratar esos datos para un fin incompatible, aunque acuda a otro supuesto de legitimación. Y es que, al tener que cumplirse con ambos preceptos, además de encontrar ese nuevo fundamento de legitimación para realizar el tratamiento ulterior de datos, deberá también cumplirse con el requisito de compatibilidad de la finalidad[678].

---

[676] Además el GA29 señala que el hecho de que los fines sean explícitos también contribuye a que el responsable genere evidencias al plasmarlos, de forma que luego le ayude a probar que ha cumplido con este principio. *Ibídem*, págs. 16 y 18.

[677] *Opinion 3/2013 on purpose limitation*, *op. cit.*, págs. 10 a 11. Así lo indica la Sentencia del TJUE de 20 de mayo de 2003, *Rechnungshof/Österreichischer Rundfunk* y otros C-465/00, C-138/01 y C-139/01, EU:C:2003:294, apdo. 65.

[678] Si bien el GA29 matiza que esto no implicará que no pueda cambiarse la finalidad inicial del tratamiento pero para ello, deberá realizarse un análisis de todos los factores, entre los que se incluirá las medidas de protección adoptadas, así como si existe una base legal para perseguir esa finalidad. *Opinion 3/2013 on purpose limitation, op. cit.*, pág. 36. En el Reino Unido, los principios de calidad enunciados en el artículo 6 de la Directiva 95/46/CE, así como los principios relativos a la legitimación del tratamiento de los datos del artículo 7 y los que se refieren a las categorías especiales de datos del artículo 8 se incluyen en varios anexos a la Ley inglesa. En el Anexo 1 se desglosan, lo que la Ley inglesa denomina, "principios de la protección de datos", entre los que aparecen los relativos a la calidad. El primero de estos principios que establece la ley inglesa es el que la Directiva 95/46/CE establece en el artículo 6.1.a): "que los datos sean tratados de manera leal y lícita". Sin embargo, se añade en la ley inglesa que "en concreto, no se podrán tratar (los datos) a no ser que (a) al menos una de las condiciones del Anexo 2 se cumpla y (b) en el caso de categorías especiales de datos, al menos una de las condiciones del Anexo 3 se cumpla". Lo que recogen estos anexos son los presupuestos que legitiman los tratamientos de datos establecidos en la Directiva 95/46/CE en sus artículos 7 y 8. Por tanto, se están conectando dos principios, de forma que para que se considere que un tratamiento respete el principio de calidad debe respetar el principio de legitimación. No es este el criterio de la Directiva 95/46/CE, que establece todos estos principios de forma independiente. Esto implica una limitación de los mismos, una forma de vaciar el contenido del principio de calidad, al que se proporciona un contenido ajeno perteneciente a otros principios y que no permitirá una interpretación autónoma de los mismos. También lo interpreta así KORFF, aunque especifica que la autoridad de control

La noción de incompatibilidad ha dado lugar a diversas interpretaciones, ya que lo único que aporta el artículo 6.1.b) Directiva 95/46/CE es que no se debe considerar incompatible el tratamiento de datos con fines históricos, estadísticos o científicos, siempre que los Estados establezcan las garantías oportunas[679]. Como se trata de un concepto jurídico indeterminado, el GA29, en cumplimiento de su labor interpretativa, ha indicado lo que considera como incompatible[680].

El hecho de que los fines sean diferentes no implica que sean incompatibles, sino que debe realizarse un análisis del caso concreto. Para encontrar un equilibrio entre la constante evolución de la sociedad y la protección de los datos personales, el GA29 apuesta por un test de compatibilidad, que atienda más a criterios sustantivos que a criterios formales[681].

El GA29 proporciona algunos factores clave que ayudarán a llevar a cabo este test de compatibilidad: la relación entre los fines de la recogida y del tratamiento ulterior; el contexto en el que se recogen los datos y las expectativas razonables que pueden tener los interesados respecto al tratamiento ulterior; la naturaleza de los datos y el impacto del tratamiento ulterior en los interesados; las medidas de protección aplicadas por el responsable para asegurar el tratamiento leal y prevenir cualquier impacto perjudicial en los interesados[682].

Respecto al hecho de considerar compatible el tratamiento de datos con fines históricos, estadísticos o científicos, el GA29 estima que no puede considerarse como una

---

inglesa expresa en su guía, que el hecho de cumplir con alguno de los supuestos que legitiman el tratamiento no es garantía de que el tratamiento sea leal y lícito, ya que la lealtad y la licitud deben examinarse de forma separada. D. KORFF, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Contract _r: JLS/2008/C4/011 – 30-CE-0219363/00-28, Country Studies, A.6-United Kingdom, op. cit.*, págs. 17 a 20, 23 y *The guide to data protection, op. cit*, pág. 44.

[679] *Commission Staff Working Paper, Impact assessment accompanying the document Regulation of the European Parliament […], op. cit., Annex 2*, pág. 25.

[680] *Opinion 3/2013 on purpose limitation, op. cit.*, págs. 23 a 27. En este sentido, cabe citar la Ley Países Bajos que ofrece también unos criterios para que el responsable pueda evaluar cuando debe considerarse incompatible la nueva finalidad: la relación entre la finalidad del tratamiento que se pretender realizar y la finalidad original; la naturaleza de los datos afectados; las consecuencias del tratamiento; la forma en la que los datos se han obtenido y las garantías que se han puesto en marcha respecto al interesado (art. 9.2 Ley Países Bajos).

[681] *Opinion 3/2013 on purpose limitation, op. cit.*, págs. 23 a 27.

[682] *Ibídem.*

excepción general al requisito de compatibilidad. Por lo tanto, el grupo entiende que deberán tenerse en cuenta todas las circunstancias que rodeen a este tratamiento de datos para determinar si es compatible o no y deberá hallarse el supuesto de legitimación en el que encaje este tratamiento, de entre los que establece el artículo 7 Directiva 95/46/CE[683]. Asimismo, para poder considerar compatibles con la finalidad inicial, estos tratamientos de datos deberán respetar las garantías que los Estados miembros deben adoptar en sus legislaciones[684].

4.1.3. Principio de calidad stricto sensu

Los datos deben ser adecuados, pertinentes y no excesivos para los fines para los que se traten (art. 6.1.c) Directiva 95/46/CE)[685]. Además los datos deben ser exactos y actualizados (art. 6.1.d) Directiva 95/46/CE). Estos requisitos que deben cumplirse respecto a los datos que se manejan son los que parecen responder más a una obligación de asegurar una calidad en los datos. Por un lado, la calidad implica un esfuerzo por obtener la mínima información, de forma que sólo se trate aquella que sea estrictamente

[683] Como indica el GA29, hay que tener en cuenta los Considerandos 29 y 40 Directiva 95/46/CE. En el Considerando 29 se precisa que "por lo general" no debe estimarse incompatible este tratamiento ulterior de datos con los fines para los que se recogieron los datos. Se exige que los Estados miembros establezcan las garantías adecuadas que deben impedir que los datos utilizados lo sean para tomar medidas o decisiones contra las personas. El artículo 11.2 Directiva 95/46/CE permite que no sea necesario cumplir con la obligación de información al interesado cuando el tratamiento tenga esta finalidad estadística, de investigación histórica o científica. El Considerando 40 que se refiere a esta disposición explica esta concreta excepción al deber de informar, al considerar que este tratamiento es susceptible de que implique esfuerzos desproporcionados. Además, el Considerando especifica que pueden tomarse en consideración, como factores para determinar si nos encontramos ante un supuesto que implique esfuerzos desproprocionados, el número de interesados, la antigüedad de los datos y las posibles medidas compensatorias. Por tanto, esta posibilidad no debería aplicarse automáticamente, ni siquiera para el tratamiento con estos concretos fines y habría que hacer la valoración de las circunstancias que envuelvan al tratamiento para poder dilucidar si cabe que se excepcione el deber de información. De la misma forma, deberán valorarse las garantías adoptadas para establecer si es posible considerar que se está ante un tratamiento ulterior compatible con los fines iniciales del tratamiento. *Opinion 3/2013 on purpose limitation*, *op. cit.*, pág. 28.

[684] A modo de ejemplo, la Ley francesa permite la conservación de datos más allá de la duración necesaria para la finalidad si estos se tratan para fines históricos, estadísticos o científicos. Las salvaguardias adoptadas por este Estado son las condiciones establecidas en la ley sectorial que regularía estas finalidades (*L. 212-3 du Code du patrimoine*), de forma que el tratamiento deberá limitarse por lo establecido en esta regulación (art. 36 Ley francesa). El GA29 establece diferentes tipos de posibles salvaguardias que se centran en el concepto de separación funcional. Esta noción implica que los datos utilizados para este tipo de fines no deben utilizarse para tomar decisiones sobre los individuos afectados. Para conseguir este objetivo, el responsable debe adoptar las medidas de seguridad necesarias para garantizar esta separación funcional, lo que habitualmente supondrá la utilización de métodos de obtención del anonimato o pseudo-anonimato. *Opinion 3/2013 on purpose limitation*, *op. cit.*, págs. 30 a 32.

[685] Hay que recordar que la Sentencia del TJUE de 20 de mayo de 2003, *Rechnungshof/Österreichischer Rundfunk* y otros C-465/00, C-138/01 y C-139/01, EU:C:2003:294, ha reconocido efecto directo a este precepto 6.1.c) Directiva 95/46/CE.

necesaria para lograr el fin perseguido. Por otro lado, la calidad implica tener una información que responda a la realidad y que sea suficiente para asegurar el fin perseguido.

Lo que se persigue es, por tanto, no tener ni más ni menos información, sino sólo la necesaria para obtener el fin que se quiere lograr con el tratamiento y que esa información sea útil y fidedigna[686]. La Directiva 95/46/CE, además, exige que se adopten las medidas razonables para que los datos inexactos o incompletos sean suprimidos o rectificados[687].

4.1.4. Principio de conservación limitada

Por último, los datos deberán ser conservados de una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente (art. 6.1.e) Directiva 95/46/CE)[688]. Mediante esta disposición se pretende que los datos no se conserven más allá de lo necesario o, al menos, si se conservan, sea de forma que no se permita identificar a los interesados, es decir, que se transformen los datos en anónimos.

Esta obligación de limitar la conservación de los datos deberá conjugarse con las obligaciones legales que tengan los responsables de preservar estos datos[689]. Esto originará no pocos problemas para delimitar los plazos de conservación de los datos. La Directiva 95/46/CE también indica que los Estados miembros establecerán garantías para

[686] La Ley eslovena obliga al responsable a verificar la exactitud de los datos mediante la solicitud de un documento de identidad o similar al interesado (art. 18.2 Ley eslovena).
[687] En lo que respecta a la obligación relativa a mantener los datos exactos y actualizados hay que resaltar lo previsto en la Ley inglesa que, en el caso de que el interesado notifique al responsable que el dato no es exacto, bastará que el responsable indique que el interesado ha efectuado esta observación y, por tanto, no se obliga al responsable a llevar a cabo la modificación del datono (Anexo 1 Ley inglesa). En la Ley austríaca, el resonsable debe probar que los datos son correctos, a no ser que provengan directamente del interesado (parágrafo 27.2 Ley austríaca).
[688] En la Ley francesa se contempla esta obligación y además se asegura el control de la misma ya que se obliga al responsable a que en el trámite de notificación de los tratamientos a la autoridad de control se indique el plazo en el que se conservarán los datos tratados (arts. 30.5 y 36 Ley francesa).
[689] Cuando finalice el fin que motiva el tratamiento, la Ley eslovena establece que los datos deberán ser suprimidos, destruidos, bloqueados o convertidos en anónimos, a no ser que una ley establezca que se puedan mantener (art. 21 Ley eslovena). La posibilidad de conservación por parte del responsable para cumplir la ley, así como también por parte del responsable y encargado para poder hacer frente a posibles responsabilidades se contempla en la legislación española (arts. 8.6 y 22 RLOPD).

que los datos personales se puedan conservar durante un plazo más largo cuando los fines sean históricos, estadísticos o científicos.

4.2. Atención de los derechos del interesado

Los derechos de acceso, rectificación, supresión, bloqueo o el de no verse sometido a una decisión automatizada, representan el poder de control que ostenta el titular de los datos respecto al tratamiento de datos. El responsable del tratamiento debe responder al ejercicio de estos derechos pero, de nuevo se encontrará ante diferencias en las legislaciones nacionales. La amplia regulación de la Directiva 95/46/CE ha dado pie a estas divergencias, especialmente, como es normal, en los procedimientos para ejercer los derechos, ya que su regulación quedaba en manos de los Estados miembros[690].

4.2.1. El derecho de acceso

El requisito preliminar para poder ejercer el poder de control sobre los datos personales es que el interesado tenga conocimiento de que existe un tratamiento de datos personales. Por eso, el principio de transparencia se ensalza en la regulación del derecho a la protección de datos que ya hemos visto es inherente a los deberes de información, calidad[691] y notificación. El derecho de acceso es una pieza más de este principio, de forma que quiere asegurar que el interesado tenga la capacidad de poder interpelar al responsable para que le proporcione la información sobre el tratamiento. Su relevancia se comprueba con la mención que realiza la Carta UE: "toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación" (art. 8.2 *in fine* Carta UE).

Sin embargo, este derecho va más allá de la simple obtención de información, ya que permite rectificarla y solicitar su supresión o bloqueo si el tratamiento no se ajustara a lo establecido en la Directiva 95/46/CE (art. 12.b Directiva 95/46/CE). Estas facultades

[690] *Commission Staff Working Paper, Impact assessment accompanying the document Regulation of the European Parliament […], op. cit., Annex 2,* págs. 32 a 34.
[691] El derecho de acceso se conecta con el principio de calidad, al indicar la Directiva 95/46/CE, que permitirá al interesado verificar la exactitud y la licitud del tratamiento (Considerando 41 Directiva 95/46/CE).

están conectadas con los principios de calidad, de forma que serían la forma en la que los interesados podrían forzar el cumplimiento de los mismos por parte del responsable.

La asignación de la obligación de atender este derecho se realiza expresamente al responsable del tratamiento[692], si bien algunas leyes han regulado la posibilidad de que los interesados se dirijan al encargado del tratamiento o que pueda existir un intermediario entre el interesado y el responsable[693].

La Directiva 95/46/CE recoge el contenido de la información que deberá proporcionarse al interesado cuando ejerza el derecho de acceso. En primer lugar, el responsable deberá confirmar si existe o no tratamiento. Es decir, aunque no tratara ningún dato personal del interesado, el responsable deberá contestar la solicitud del titular de los datos. El responsable también debe informar sobre los fines del tratamiento, las categorías de datos tratados, los destinatarios o las categorías de destinatarios a quienes se comunican los datos, los datos objeto de los tratamientos y toda la información disponible

[692] Como indica HEREDERO HIGUERAS durante el proceso de elaboración de la Directiva 95/46/CE se valoró incorporar esta disposición en un precepto que conformara el estatuto del responsable del tratamiento. M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, págs. 107 y respecto a este artículo 12, pág. 145.

[693] Cuando el tratamiento lo lleva a cabo un sujeto distinto al responsable (un encargado del tratamiento) puede ser más factible que el interesado se diriga a este sujeto, en lugar de al responsable al ejercer su derecho de acceso. Esta posibilidad se ha regulado en algunas leyes nacionales. Así, por ejemplo, en la Ley austríaca se establece que cuando un interesado se dirija a ejercer su derecho de acceso al proveedor de servicios que actúa por cuenta del responsable porque entiende que se trata del responsable, este proveedor de servicios deberá redirigir la solicitud al responsable e informar al interesado (parágrafo 26.10 Ley austríaca). También se incluye regulación que contempla estos supuestos en el artículo 12.4 Ley checa, artículo 11.4 Ley de Liechtenstein y como se verá en la legislación española (art. 26 RLOPD). Por otro lado, también en algunas leyes se dispone, en determinados supuestos, la posibilidad de que exista una intermediación entre el interesado y el responsable ante el que se quiere ejercer el derecho. Como ejemplo se puede citar la Ley portuguesa que establece que en los casos en los se quiera ejercer un derecho de acceso con relación a un tratamiento de datos que persiga fines periodísticos o artísticos o de expresión literaria o a un tratamiento de datos relativos a fines de seguridad del estado o prevención penal o investigación se llevará a cabo a través de la autoridad de control (art. 11 apartados 2 y 3 Ley portuguesa). Además en el marco de los datos de salud, el ejercicio del derecho de acceso podrá realizarse mediante el médico que elija el interesado (art. 11.5 de la Ley portuguesa). Respecto a los datos sanitarios también establecen esta posibilidad de intermediación mediante el médico el artículo 13.4 Ley rumana y el artículo 11.3 Ley de Liechtenstein. Hay que decir que, respecto a este último ejemplo, en el proceso de elaboración de la Directiva 95/46/CE se introdujo en las primeras versiones la habilitación para que los Estados previeran que el acceso a los datos de salud se realizara a través del médico de confianza del interesado, disposición que se inspiraba algunas leyes nacionales (francesa, luxemburguesa, danesa y portuguesa), texto que finalmente se eliminó de la versión final del articulado de la directiva pero que permaneció en el Considerando 42. En el mismo se especifica que los Estados miembros podrán precisar que el acceso a los datos de carácter médico únicamente puedan obtenerse a través de un profesional de la medicina. M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, págs. 144, 151.

sobre el origen de los datos y la lógica utilizada en los tratamientos[694]. En algunas leyes nacionales se ha ampliado esta información[695].

La información sobre la lógica se centra en los tratamientos automatizados y se precisa que, al menos, deberá proporcionarse en los casos de decisiones individuales automatizadas que establece el artículo 15 Directiva 95/46/CE. Durante el proceso de elaboración de la Directiva 95/46/CE, las empresas de publicidad formularon reparos al formar parte de su práctica la utilización de algoritmos para seleccionar las personas a las que destinar los mailings.

Estas empresas alegaron que estos algoritmos eran parte de su secreto comercial y que, si se desvelaban a raíz de una petición de los titulares de los datos de conocer la lógica del tratamiento, podrían ser aprovechados por los competidores y que además requerirían de un esfuerzo considerable para explicarlos a los interesados. Por eso, se incluyó en el Considerando 41 una salvedad respecto a esta información, de forma que el ejercicio del derecho de acceso no deberá menoscabar el secreto de los negocios ni la propiedad intelectual y, en particular, el derecho de autor que proteja el programa informático. Ello, no obstante, se añadió que no debe suponer que se deniegue cualquier información al interesado. Por tanto, deberá entregarse la información que no menoscabe directamente los intereses comerciales señalados[696]. Esta previsión tiene especial relevancia en virtud de la evolución de los sistemas de análisis de la información digital que se fundamentan en el diseño de complejos algoritmos, de gran valor comercial.

---

[694] Respecto a los datos objeto del tratamiento y el origen de los datos, se indica que el responsable debe comunicar en forma inteligible los datos, lo que deja entrever que la información deberá facilitarse en algún soporte que permita al interesado que pueda aprehender de forma clara y comprensible los datos tratados.

[695] Por ejemplo, la Ley austríaca además obliga a dar información sobre la base jurídica a la que se ha acogido el responsable para legitimar la utilización de los datos personales (parágrafo 26.1 Ley austríaca). La Ley francesa obliga también a informar sobre las transferencias de datos a países no miembros de la UE (art. 39.I.3 Ley francesa). También contemplan aspectos adicionales: Sección 15 Ley húngara, artículo 19.4 Ley croata, artículo 15.3.3 Ley letona, artículo 23.1.2 Ley lituana y artículo 11.2.b Ley de Liechtenstein. Resaltar además la particular regulación del derecho de acceso en las Leyes noruega e islandesa, donde se establecen dos tipos de derecho: el derecho de acceso a información general del tratamiento y el derecho de acceso, como tal. El primero lo puede ejercer cualquier persona y se refiere a aspectos más generales del tratamiento y el segundo sería el que corresponde con el regulado por la Directiva 95/46/CE (art. 18 Ley noruega y arts. 16 y 18 Ley finlandesa).

[696] M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, págs. 144 a 145. Este Considerando 41 se ha incorporado, por ejemplo, en la Ley inglesa que especifica que la información que se brinde al interesado acerca de la lógica seguida en la toma de decisiones automatizadas no se referirá a información que constituya secreto empresarial (Sección 8.5 Ley inglesa).

Respecto al procedimiento que debe seguir el responsable para atender el derecho deberá tener en cuenta que la Directiva 95/46/CE exige que se garantice el ejercicio por parte del interesado libre, sin restricciones, con una periodicidad razonable y sin retrasos ni gastos excesivos[697]. El TJUE ha resaltado la importancia de este derecho, no sólo como instrumento para ejercer los otros derechos del artículo 12 Directiva 95/46/CE, sino para poder ejercer el derecho al recurso (arts. 22 y 23 Directiva 95/46/CE)[698]. En este sentido, el TJUE ha estimado que el alcance de este derecho puede abarcar también datos anteriores al momento de ejercerlo[699]. Asimismo, respecto a los gastos también se ha pronunciado el Alto tribunal, que ha indicado que incumbe a los Estados miembros decidir si exigen el pago de los mismos pero que no deberían ser mayores del coste de la comunicación de datos[700].

La Directiva 95/46/CE especifica que los datos objeto del tratamiento y la información sobre el origen se comunicarán, en forma inteligible. El TJUE ha interpretado que son los Estados miembros quienes deben determinar la forma material concreta que debe adoptar esa comunicación, siempre que se cumpla el requisito de que

[697] Estos aspectos se han recogido de forma diversa en las legislaciones nacionales. En casi todas las leyes se disponen plazos para responder al ejercicio de los derechos. No obstante, no se establecen plazos concretos en la Ley maltesa, en la que sólo se indica respecto al derecho de acceso que debe contestarse sin excesiva tardanza (art. 21.1 Ley maltesa). En las leyes que sí establecen plazos para responder, si bien la norma general suelen ser treinta días, hay otros plazos más cortos (como los cinco días laborables que fija el artículo 19.3 Ley estonia) o más largos (tres meses en artículo 28.2 Ley finlandesa). En ocasiones también se establecen varios plazos, como en la Ley eslovena donde se fija un máximo de quince días para manifestar las razones de la negativa o de treinta días si lo que hace el responsable es atender el derecho (art. 31.2 y .3 Ley eslovena). En la Ley chipriota se fija un plazo de cuatro semanas para contestar la solicitud del derecho de acceso y de 15 días para contestar la solicitud de oposición (arts. 12.3 y 13.1 Ley chipriota). En la legislación española se establece un plazo de un mes para resolver la solicitud y de diez días para hacerla efectiva si se estimara la misma (art. 29, apartados 1 y 2 RLOPD). Algunas leyes también han establecido limitaciones temporales para el ejercicio de este derecho (art. 31.1 Ley eslovena, art. 15.4 Ley letona y art. 15.3 LOPD). La Ley chipriota dispone que, para ejercer los derechos de acceso y oposición, se debe pagar un importe que se devolverá si el responsable o la autoridad admiten la solicitud de rectificación o supresión, en cuyo caso además se exige que el responsable entregue una copia del tratamiento rectificado (art. 14 Ley chipriota). Se establece la posibilidad de cobrar el coste de la copia que se entregue al interesado de los datos en el artículo 39.I Ley francesa, artículo 31.5 Ley eslovena y artículo 20 Ley estonia. Se podrá repercutir un cargo si el derecho de acceso se ejerce en un intervalo de menos de un año según el artículo 26.3 Ley finlandesa y el artículo 25.1 Ley lituana.

[698] Sentencia del TJUE de 7 de mayo de 2009, *College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer*, C-553/07, EU:C:2009:293, apdos. 51 a 55. Ver Capítulo VII. Asimismo, cabe citar la utilización del derecho de acceso a los antecedentes penales por empleados o candidatos a algún puesto obligados por su potencial empleador. En este sentido, la Ley belga establece como infracción el hecho de obligar a una persona a que entregue los datos obtenidos como resultado al ejercitar su derecho de acceso (art. 39.6 Ley belga).

[699] Si bien matiza el TJUE que el artículo 12.a) Directiva 95/46/CE debe relacionarse con el artículo 6.1.e) Directiva 95/46/CE, de forma que el responsable no podrá conservar los datos durante un período superior al necesario para los fines para los que se recogieron los datos o para los que se traten ulteriormente. *Ibídem*.

[700] Sentencia del TJUE de 12 de diciembre de 2013, *X*, C-486/12, EU:C:2013:836, apdos. 22, 26, 28-31.

sea inteligible[701]. Que sea inteligible, según el tribunal, equivale a que permita a los interesados conocer esos datos y comprobar que son exactos y tratados de conformidad con la Directiva 95/46/CE. Ello no implica que el interesado tenga un derecho a obtener copia exacta de la información, sino que se puede haber alterado esa información para que el interesado no pudiera acceder a información distinta de sus datos personales[702].

En el mismo artículo 12 Directiva 95/46/CE, bajo el título del derecho de acceso también se incluye la regulación del derecho a obtener del responsable la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la directiva, en particular si los datos están incompletos o son inexactos. Además, estos derechos implican que si los datos se han comunicado a terceros, el responsable deberá notificar a estos terceros toda rectificación, supresión o bloqueo efectuado, si no resulta imposible o supone un esfuerzo desproporcionado[703].

Pese a que la Directiva 95/46/CE incluye la rectificación, la supresión y el bloqueo en el derecho de acceso, en la mayoría de las legislaciones de los Estados miembros se configuran como derechos autónomos del de acceso e incluso en algunas de estas normas se añaden nuevas modalidades de derechos[704].

En algunas leyes nacionales se establece que el responsable deba rectificar o suprimir de oficio los datos, lo que entiendo que cumple con lo establecido en el principio de calidad, en el artículo 6.1.d) Directiva 95/46/CE, ya comentado aunque se ubique en la

[701] Sentencia del TJUE de 17 de julio de 2014 *YS*, C-141/12 y C/372/12, EU:C:2014:2081, apdo 57.
[702] Hay que tener en cuenta que, en el asunto que se trataba se determinó, que una parte de los datos que se incluían en la información que solicitaba el interesado, mediante el ejercicio del derecho de acceso, no eran datos personales y, en consecuencia, no podía acceder a ellos. *Ibídem*, apdos. 58-60.
[703] Esta comunicación que según lo que dispone la Directiva 95/46/CE debería ser solicitada por el interesado, por regla general en las leyes nacionales se establece como una obligación que tiene el responsable, sin requerir que el interesado se lo solicite. Como ejemplo, en la regulación del derecho de rectificación, baste citar el artículo 16.4 LOPD y el artículo 29.3 Ley finlandesa. No obstante, se contempla que sólo a petición del interesado informará el responsable a los destinatarios de los datos a los que hubiera suministrado los datos en el artículo 32.2 Ley eslovena y en el artículo 28a Ley búlgara.
[704] En la Ley chipriota la solicitud de rectificación, supresión o bloqueo (y además también se añade la solicitud de suspensión del tratamiento o de no comunicación) se incluye en el derecho de oposición (art. 13.1 Ley chipriota) y no en el derecho de acceso. En la Ley eslovena se añade al derecho de rectificación, bloqueo, supresión y oposición, el derecho de adición (art. 32 Ley eslovena). En la Ley Países Bajos el ejercicio del derecho de acceso permite que la persona que lo haya ejercido pueda requerir al responsable que rectifique, complete, suprima o bloquee los datos si estos fueran inexactos, incompletos o inadecuados a la finalidad del tratamiento o se trate de otra forma que infrinja la legislación. La solicitud debe incluir la modificación que se solicita (art. 36.1 Ley Países Bajos).

regulación de los derechos de los interesados[705]. Como ya se ha indicado, los principios de calidad y el derecho de acceso están estrechamente relacionados, ya que lo que implica este último, es la forma de obligar al responsable a cumplir con los primeros. En este sentido, por ejemplo, la operación de bloqueo ha sido regulada de forma específica en las leyes nacionales y se utiliza indistintamente para ambos aspectos de la regulación, calidad y derechos[706].

Estos derechos de acceso, rectificación, supresión y bloqueo pueden ser limitados por los Estados miembros mediante dos vías. La primera será mediante la adopción de una medida legal que sea necesaria para la salvaguardia de los aspectos que determina el artículo 13.1 Directiva 95/46/CE[707]. La segunda vía será específica para la limitación de

[705] Así lo establece el artículo 4.4 LOPD en sede del principio de calidad y el artículo 20 Ley croata. Además cabe destacar la regulación de las Leyes austríaca y de los Países Bajos, en las que se alude a la posibilidad de que los soportes donde figuran los datos no permitan la modificación o la supresión de los mismos (parágrafo 27.6 Ley austríaca y artículo 36.4 Ley Países Bajos).

[706] En la Ley lituana, además de la posibilidad de solicitar la rectificación o la destrucción de los datos se menciona la opción de suspender el tratamiento cuando vulnere la ley (art. 23.1.3 Ley lituana). La Ley húngara establece los supuestos en los que se suprimirán o se bloquearán los datos (Sección 17 Ley húngara). La Ley maltesa incluye una definición de bloqueo que es la operación consistente en la suspensión de la modificación de datos o la suspensión o restricción de entrega de la información a un tercero cuando esta entrega esté suspendida o restringida de acuerdo con lo establecido en la Ley maltesa (art. 2 Ley maltesa) y también se hace referencia al bloqueo en la definición de cancelación que establece la legislación española (art. 5.1.b RLOPD).

[707] Como ejemplo de la regulación incorporada en las legislaciones nacionales de la vía que permite el artículo 13.1 Directiva 95/46/CE, citar la Ley inglesa que en su regulación del derecho de acceso se refiere a la posibilidad de que el responsable se pueda negar a proporcionar la información solicitada si ello conlleva entregar al interesado solicitante información relacionada con otro individuo. Hay que entender que utiliza el supuesto establecido en el artículo 13.1.g) Directiva 95/46/CE relativo a la posibilidad de limitar el artículo 12 Directiva 95/46/CE en virtud de la protección de los derechos y libertades de otras personas. Se establecen, no obstante, varias excepciones: si el individuo afectado hubiera consentido esta comunicación de datos a la persona que ejerce el derecho o si fuera razonable que cumpla con esta solicitud sin el consentimiento del individuo. Para poder valorar cuando será razonable que el responsable pueda cumplir con la solicitud sin el consentimiento del individuo, la ley indica algunos aspectos que deben tenerse en cuenta: cualquier deber de confidencialidad que pudiera haberse suscrito con el individuo afectado, los pasos que el responsable hubiera realizado para solicitar el consentimiento, si el individuo era capaz de otorgar su consentimiento y si hubiera un rechazo expreso a otorgar el consentimiento por parte del individuo. Además tampoco se podrá negar el responsable en virtud de esta alegación si pudiera proporcionar al solicitante la información sin tener que identificar a la persona, por ejemplo eliminando los datos que pudieran identificarlo (Sección 7.4 y 5 Ley inglesa). Como indica KORFF, la ley no hace referencia como argumentos para no proporcionar la información el hecho de que esa información pudiera perjudicar a este tercero, lo que, en realidad, es el único argumento que estaría en línea con la regulación establecida en la directiva. D. KORFF, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Contract _r: JLS/2008/C4/011 – 30-CE-0219363/00-28, Country Studies, A.6-United Kingdom, op. cit.*, pág. 49. Otros ejemplos de disposiciones que han aprovechado esta vía para limitar el derecho de acceso son los artículos 26.2 y 34 Ley búlgara, el artículo 20 Ley estonia, el artículo 36 Ley eslovena, el artículo 15.1 Ley letona, el artículo 23 Ley lituana, el artículo 12.3 Ley de Liechtenstein. Entre los supuestos que establece el artículo 34 Ley polaca que permitiría que el responsable pudiera rechazar proporcionar la información solicitada en ejercicio del derecho de acceso se incluye la referencia a que ello supusiera divulgar información confidencial, supuesto que no se encuentra claramente en el artículo 13.1 Directiva 95/46/CE.

este artículo 12 Directiva 95/46/CE, mediante una disposición legal y para el caso de que los datos se traten para fines de investigación científica o se archiven durante un período que no supere el tiempo necesario para elaborar estadísticas (art. 13.2 Directiva 95/46/CE[708]).

4.2.2. El derecho de oposición

Otro derecho que establece la Directiva 95/46/CE es el de oposición (art. 14 Directiva 95/46/CE). Este derecho no se configura como un derecho general a oponerse a todo tipo de tratamiento de datos, sino que se obliga a los Estados miembros a que lo reconozcan, al menos, en los supuestos especificados que son: cuando se refiera al tratamiento de datos para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público (contemplado en el artículo 7.e) Directiva 95/46/CE); el supuesto que permite el tratamiento para satisfacer el interés legítimo del responsable del tratamiento o por el tercero a quien se puedan comunicar los datos (previsto en el artículo 7.f) Directiva 95/46/CE) y cuando sean tratamientos con fines de prospección comercial[709].

En los dos primeros supuestos, el interesado debe justificar su oposición por razones legítimas propias de su situación particular. No obstante, hay que decir que, en estos casos, se permite a los Estados miembros que establezcan mediante la legislación nacional la imposibilidad de que el interesado ejerza este derecho. Esta posibilidad de limitación se añadiría a las que ya tienen los Estados vía el artículo 13 Directiva 95/46/CE[710].

[708] Este artículo 13.2 Directiva 95/46/CE se incluyó en la directiva como resultado de las observaciones formuladas por los organismos de estadística respecto a otros preceptos. De esta forma, estos organismos indicaron durante la elaboración de la directiva que debía entenderse que la prohibición de tratar datos de forma incompatible con los fines del momento de recogida de estos datos, debía entenderse en el ámbito de los fines estadísticos o de investigación sólo si se utilizaran en apoyo de medidas o decisiones adoptadas en contra del titular de los datos. Esta idea, recogida, como se ha visto anteriormente, en el Considerando 29 respecto al artículo 6.1.b) Directiva 95/46/CE también se incluye en este artículo 13.2. M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, págs. 151 a 152.

[709] Si bien durante el proceso de elaboración de la Directiva 95/46/CE inicialmente se reguló este derecho como un derecho general, inspirado en la ley francesa que así lo reconocía. M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, págs. 153 a 154.

[710] Esta previsión resulta algo confusa, ya que por un lado, el artículo establece un mínimo de supuestos en los que debe reconocerse este derecho y, por el otro, se permite que se invaliden, lo que implica que los Estados miembros, al final, no están obligados a establecer el derecho. Quizás, esta confusión se explique por el origen de la disposición, que ya se ha indicado que se inspiró en la Ley francesa y que sólo

En el caso relativo a los tratamientos con fines de prospección comercial[711] se presentan varias situaciones, en las que las obligaciones del responsable difieren. Así, cuando el responsable prevea un tratamiento destinado a esta finalidad, el interesado podrá oponerse, previa petición y sin gastos a este tratamiento. Se establece para este supuesto que los Estados miembros adopten las medidas necesarias para garantizar que los interesados conozcan la existencia de este derecho, lo que parece lógico porque, en caso contrario, su utilidad sería muy relativa.

Si se quieren comunicar los datos a un tercero (se entiende, aunque no lo especifique la Directiva 95/46/CE, que para fines de prospección) se debe informar al interesado antes de la primera comunicación. En este caso de comunicación y también si se quieren utilizar los datos en nombre de terceros a efectos de prospección comercial debe ofrecerse al interesado expresamente el derecho de oponerse, sin gastos[712].

En algunas leyes se ha previsto la posibilidad de que los responsables del tratamiento conserven los datos mínimos necesarios para no volver a incorporar los datos del interesado que hubiera ejercido el derecho de oposición en las listas de destinatarios de información comercial[713].

---

contemplaba un límite a este derecho que era que el tratamiento estuviera regulado por disposición reglamentaria. Este límite es el que parece que se refleja en este precepto, artículo 14.a) Directiva 95/46/CE, cuando indica "salvo cuando la legislación nacional disponga otra cosa" y que se especifica en el Considerando 45, cuando precisa que los Estados miembros tienen la posibilidad de establecer disposiciones nacionales contrarias. *Ibídem.*

[711] Aunque por ejemplo la Ley Países Bajos amplía la regulación del derecho de oposición además de a tratamientos de datos con fines comerciales también a tratamientos con fines de caridad (*charitable purposes*) (art. 41.1 Ley Países Bajos).

[712] De esta previsión, el legislador austríaco dedujo que el tercero en nombre del que se realicen las acciones de prospección no podía adquirir la cualidad de responsable y, por eso, se obligaba al responsable del tratamiento que realizara la tarea informar al interesado. Esta previsión no se encuentra en la parte dedicada a la regulación del derecho de oposición sino como una obligación de identificación del responsable (parágrafo 25.2 Ley austríaca). Esta sería una interpretación divergente, por ejemplo, con la que la ley española ha realizado, al entender, como ya se indicó anteriormente que aquel sujeto en beneficio del que se realiza una acción comercial es un responsable del tratamiento, aunque no tenga acceso material a los datos. En lo que respecta a la regulación de la Ley austríaca del derecho de oposición esta se encuentra en el parágrafo 28 Ley austríaca.

[713] Se trata de las conocidas como "listas robinson". Así en la Sección 11 Ley inglesa se establece el derecho de oposición al tratamiento de datos con fines de marketing directo. Como indica D. KORFF la autoridad de control inglesa (el ICO) interpreta que la supresión de los datos no puede ser completa ya que deben quedar los datos mínimos para que el responsable pueda garantizar que en el futuro esa persona no volverá a ser incluida en las listas de distribución. De esta forma el responsable deberá tener su propia lista Robinson con los datos de aquellas personas que no desean recibir comunicaciones comerciales. D. KORFF, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Contract _r: JLS/2008/C4/011 – 30-CE-0219363/00-28, Country Studies, A.6-*

El derecho de oposición persigue, de acuerdo con esta regulación de la Directiva 95/46/CE, que el interesado pueda ir en contra de un tratamiento que se considerará lícito (Considerando 45 Directiva 95/46/CE)[714]. Este hecho ha planteado si existe lo que se ha venido en conocer como el derecho al olvido, como un derecho que tendrían los interesados a solicitar la eliminación de sus datos en el contexto de Internet aunque su tratamiento fuera considerado lícito.

4.2.3. La reconducción del derecho al olvido hacia los derechos de acceso y oposición

La Audiencia Nacional planteó, en una cuestión prejudicial, al TJUE, si en virtud de los derechos de supresión y oposición (arts. 12.b) y 14.1.a) Directiva 95/46/CE), una persona podía solicitar a un gestor de un motor de búsqueda que eliminara de su lista de resultados enlaces a páginas web de terceros obtenidos a partir de la introducción en el buscador de su nombre y apellidos[715]. Estas páginas web incluían información sobre este interesado que se consideraba lícita pero que éste estimaba que le perjudicaba y, por eso, reclamaba su derecho al olvido.

El TJUE estimó que el gestor del motor de búsqueda, que era *Google*, era responsable del tratamiento de los datos necesario para llevar a cabo su actividad y, por tanto, debía atender los derechos del interesado. Una primera vía será utilizar el derecho de supresión, que exige que el tratamiento sea incompatible con la Directiva 95/46/CE, ya que ello podía resultar del incumplimiento de los principios de calidad. Así consideraba el TJUE que un tratamiento inicialmente lícito podía llegar a incumplir con estos principios con el paso del tiempo[716].

United Kingdom, op. cit., pág. 53. En la legislación española se ha regulado también la elaboración de listas robinson que los responsables deberán consultar antes de poder realizar las comunicaciones comerciales (arts. 48 y 49 RLOPD).

[714] M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, pág. 154.

[715] Sentencia del TJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2014:317, apdos. 92 ss. Ver Capítulo VIII.

[716] En palabras de la profesora y exdirectora de la ACPD, Esther Mitjans Perelló, "el derecho al olvido es el derecho a que el pasado no se convierta en presente continuo". J. DE LA CUEVA GONZÁLEZ-COTERA, "Relato del VII Congreso Internacional sobre Internet, Derecho y Política: Neutralidad de la red y derecho al olvido", *Revista de Internet, Derecho y Política*, nº 13, Febrero 2012, pág. 88.

Otra opción es ejercer el mismo derecho de supresión o el de oposición por considerar que no se cumple con el supuesto de legitimación. Se había considerado que el supuesto al que se podía acoger el gestor del motor de búsqueda para tratar datos era el del interés legítimo (art. 7.f) Directiva 95/46/CE). Como indicaba el TJUE, el tratamiento, en este caso, debe ser legítimo durante todo el período en el que se efectúa[717]. Por tanto, el gestor del motor de búsqueda debía realizar la ponderación de, si en el momento en el que se realizaba la solicitud de ejercicio de derechos, debía primar su interés legítimo, o el derecho del interesado a eliminar el enlace. El TJUE indicó que en esta ponderación también debía tenerse en cuenta el interés del público en encontrar la información que, por ejemplo, podría prevalecer, si el afectado tuviera un papel en la vida pública[718].

Unos dos meses después de emitirse la sentencia, *Google* informaba que había recibido más de 70.000 solicitudes de eliminación de enlaces, lo que puede dar una idea de la relevancia del pronunciamiento judicial[719]. Ante la falta de criterios para realizar la ponderación, el GA29 emitió una guía con algunas pautas que aplicarían las autoridades para hacer esta valoración[720].

4.2.4. Decisiones individuales automatizadas

Otro derecho que establece la Directiva 95/46/CE, en beneficio de las personas y que deberán respetar los responsables, pese a que esta asignación no se especifique en la regulación expresamente, es el de no verse sometidas a una decisión con efectos jurídicos

[717] Sentencia del TJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2014:317, apdo. 95. El TJUE introduce, según SIMÓN CASTELLANO, la idea de la caducidad del interés legítimo para valorar si hay que conservar los datos en Internet. En virtud del funcionamiento de Internet, este autor estima necesario introducir el olvido respecto a finalidades legítimas que caducan o perecen con el paso del tiempo en el ciberespacio. P. SIMÓN CASTELLANO, *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014*, Bosch, Barcelona, 2015, pág. 258.

[718] Sentencia del TJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2014:317, apdo. 97. En este sentido VILASAU SOLANA considera que el TJUE otorga una prevalencia excesiva al derecho del afectado frente al derecho a la información de los usuarios de Internet. M. VILASAU SOLANA, "El caso Google Spain: la afirmación del buscador como responsable del tratamiento y el reconocimiento del derecho al olvido (análisis de la STJUE de 13 de mayo de 2014)", *IDP. Revista de Internet, Derecho y Política*, Número 18, págs. 16-32. UOC, http://journals.uoc.edu/index.php/idp/article/view/n18-vilasau/n18-vilasau-es (fecha consulta: 8.7.2015), pág. 24.

[719] P. SIMÓN CASTELLANO, *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014*, *op. cit.*, pág. 268.

[720] *Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12, 14/EN WP 225, 26.11.2014, Article 29 Data Protection Working Party.*

o que les afecte de manera significativa. Esta decisión, además, debe haberse fundamentado únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad[721].

Sin embargo, la Directiva 95/46/CE admite que los Estados miembros permitan que una persona pueda someterse a este tipo de decisión cuando se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que se salvaguarde su interés legítimo o que la petición de la celebración o ejecución del contrato presentada por el interesado se haya satisfecho. La persona podrá también someterse a este tipo de decisiones, si éstas se autorizan por ley en la que se establezcan medidas que garanticen el interés legítimo del interesado[722].

Además, como ya se ha comentado, respecto al derecho de acceso se especifica que este derecho no podrá menoscabar el secreto de los negocios ni la propiedad intelectual (Considerando 41 Directiva 95/46/CE). No obstante, tampoco esta protección para los responsables podrá suponer una denegación automática en virtud de estas razones.

[721] No es preciso que la decisión suponga efectos perjudiciales para el interesado, sino que basta que afecte de forma significativa al interesado. El objeto del tratamiento automatizado debe ser la evaluación de determinados aspectos de la personalidad, lo que eliminaba la actividad comercial que simplemente consistiera en enviar prospectos a una lista de destinatarios. M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, págs. 158 a 159. Como se ha indicado respecto al derecho de acceso, cuando se hacía mención de la posibilidad de conocer la lógica del tratamiento, este derecho ha adquirido especial trascendencia en el actual contexto de Internet. De forma que, si en un inicio el peligro era que las empresas realizan perfiles de los usuarios con el fin de hacerles llegar publicidad personalizada, ahora se han ampliado los riesgos de vulneración del derecho a la protección de datos por la aparición de herramientas de análisis de lo que se conoce como *big data*, es decir ingentes cantidades de información que se vuelcan a Internet. Ver Capítulo VIII.

[722] El artículo 10 Ley francesa, que regula este derecho, no contempla la posibilidad que brinda la directiva de que se pueda someter a una persona a este tipo de decisiones si se establece por una ley. Sin embargo, si admite que se someta a esta persona a la decisión si se satisface una solicitud de esta persona. Hay que tener en cuenta que fue precisamente la ley francesa la que dio origen a este precepto de la Directiva 95/46/CE. M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, pág. 157.

4.3. El deber de confidencialidad y de seguridad del tratamiento

4.3.1. El deber de confidencialidad

El deber de confidencialidad que establece la Directiva 95/46/CE es algo confuso, ya que no se equipara con lo que puede considerarse confidencialidad, tal como se define normalmente esta obligación como un compromiso de no divulgación de la información y de sigilo[723]. Bajo el título de confidencialidad del tratamiento, se describe esta obligación como la necesidad de que las personas que actúan bajo la autoridad del responsable o del encargado del tratamiento, incluyéndose a este encargado del tratamiento (se entiende que respecto al responsable) sólo podrán tratar datos a los que tengan acceso cuando se lo encargue el responsable del tratamiento (art. 16 Directiva 95/46/CE).

En consecuencia, de esta formulación se desprende más un deber de subordinación por parte de quienes están bajo la autoridad del responsable o el encargado. Sin embargo, algunas leyes nacionales han orientado su regulación hacia la concepción de una obligación de secreto[724]. Como consecuencia se ha estipulado, por ejemplo, el carácter indefinido de este deber de secreto, carácter que, en la concepción de subordinación no tendría sentido[725].

---

[723] Así se había establecido en el inicio del proceso de elaboración de la Directiva 95/46/CE. En la Propuesta de Directiva de 1990 se integraba esta obligación en el artículo dedicado a la seguridad de los datos, como una obligación que tenían las personas con acceso a los datos de no comunicarlos a terceros sin autorización del responsable. Por tanto, se había configurado como una obligación de no divulgación a terceros. M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, págs. 160 a 161. Cabe citar en este sentido la obligación de confidencialidad que la Ley finlandesa configura como un deber de no divulgación a terceros por parte de cualquier persona que acceda a los datos y que además refiere a unas categorías de datos específicas (características, circunstancias personales o situación económica de una persona) (art. 33 Ley finlandesa).

[724] Así se ha establecido en la legislación española como una obligación de secreto profesional respecto a los datos (art. 10 LOPD). La Ley portuguesa en su artículo 17 incluye una obligación de secreto profesional que deberán cumplir los responsables y las personas que accedan a los datos en cumplimiento de sus funciones. No obstante, esto no impide que, tal como especifica el mismo artículo, estas personas deban proporcionar la información si a ello les obliga la ley. La Ley Países Bajos incluye en la regulación de esta obligación que las personas autorizadas o el encargadod el tratamiento que acceden a los datos subordinados al responsable si no estén sujetas a un deber de confidencialidad por su profesión o por ley se les requerirá que traten los datos de forma confidencial, excepto cuando la comunicación se requiera por ley o sea precisa para el desarrollo apropiado de sus tareas (art. 12.2 Ley Países Bajos). La ley de Liechtenstein establece una obligación de confidencialidad que responde a la obligación de mantener secreto y que pertoca a aquellas personas que tratan datos en virtud de sus actividades profesionales, sin perjuicio de otras posibles obligaciones de confidencialidad y salvo que exista legitimación legal para transmitir datos (art. 10 Ley de Liechtenstein).

[725] Así lo establecen el artículo 10 LOPD, artículo 26.2 Ley estonia, artículo 24.4 Ley eslovena, artículo 27.1 Ley letona, artículo 30.6 Ley lituana y artículo 15.1 Ley checa.

Esta obligación de confidencialidad no debe cumplirla el responsable del tratamiento, sino las personas que actúen bajo la autoridad de éste o del encargado del tratamiento y también éste último[726]. Sin embargo, se hace alusión a la misma en este apartado del estudio, ya que su cumplimiento estará fuertemente ligado con la obligación relativa a la seguridad del tratamiento, que sí debe cumplir el responsable[727].

Además, esta disposición lo que hace es reflejar la relación de subordinación de estas personas y del encargado respecto al responsable del tratamiento, lo que tiene su incidencia en la responsabilidad frente a posibles incumplimientos de la normativa[728]. Si estas personas actúan bajo las órdenes del responsable, éste debe ser el que asuma las consecuencias de estas decisiones. Al ser el responsable quien decide qué personas se encargan del tratamiento, debe ser quien se ocupe de que la gestión que realicen estas personas sea la adecuada[729].

---

[726] La Ley eslovena establece la obligación de secreto para todos los funcionarios, empleados y cualquier otra persona que trabaje para personas que tratan datos (art. 24 Ley eslovena). El artículo 15 Ley checa también amplía el alcance de esta obligación hacia cualquier persona física que trate datos personales en virtud de un contrato suscrito con el responsable o el encargado u otras personas que, con el fin de cumplir obligaciones legales, accedan a los datos en las ubicaciones del responsable o del encargado.

[727] De hecho como se ha comentado previamente, este deber de confidencialidad se había integrado en un primer momento en el artículo que regulaba la obligación de seguridad. M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, págs. 160 a 161. Como ejemplo de esta integración con las medidas de seguridad, mencionar la Ley polaca que a la obligación de limitar el tratamiento sólo a las personas autorizadas por el responsable (art. 37 Ley polaca) añade que el responsable está obligado a asegurar que se pueda supervisar cuándo, a qué datos y quién ha accedido al sistema informático y a quién se proporcionan estos datos (art. 38 Ley polaca). Para ello el responsable debe mantener un registro de personas autorizadas a llevar a cabo el tratamiento y estas personas deben conservar estos datos y la forma como están protegidos de forma confidencial (art. 39 Ley polaca). También en la Ley letona se incluye la obligación que tendrá el responsable de mantener un registro de estas personas (art. 27.2 Ley letona). Y es que una medida de seguridad evidente es la de limitar el acceso a los datos a aquellas personas que lo precisen para el desarrollo de sus funciones. Esto sólo se puede realizar si se tiene el control de quienes son estas personas y su nivel de acceso. Finalmente mencionar la Ley checa que obliga a mantener la confidencialidad de los datos personales y también de las medidas de seguridad, cuya divulgación podría implicar un peligro para la seguridad de los datos (art. 15 Ley checa).

[728] La Ley luxemburguesa contempla titula con más acierto esta obligación de "subordinación" (art. 21 Ley luxemburguesa). La Ley danesa en la regulación de este deber de confidencialidad también se refiere a individuos y compañías que trabajen para el responsable o el encargado (art. 41.1 Ley danesa).

[729] En la Ley chipriota el responsable debe seleccionar para llevar a cabo el tratamiento personas que dispongan de cualificaciones apropiadas y que provean suficientes garantías con respecto al conocimiento técnico y la integridad personal para cumplir con esta obligación de confidencialidad (art.10.2 Ley chipriota). En la Ley estonia se establece que el responsable debe garantizar la formación en el área de protección de datos de las personas que tratan los datos (art. 26.3 Ley estonia). Un ejemplo del especial papel que se otorga al encargado del tratamiento en la Ley checa se refleja en esta obligación de confidencialidad. Así, en esta ley se establece que los empleados del responsable o del encargado y otras personas que traten los datos personales en virtud de un contrato con el responsable o el encargado, podrán tratar los datos personales sólo bajo las condiciones y el alcance especificado por el responsable o el encargado. Es decir, el encargado también podrá definir las condiciones y el alcance del tratamiento (art. 14 Ley checa).

Sin embargo, las personas que actúan bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, podrán tratar datos en virtud de un imperativo legal. Esto supone establecer una vía de escape para los sujetos obligados, que podrán zafarse de cumplir con las órdenes del responsable, si ello tiene como objetivo cumplir con una obligación legal de carácter imperativo[730]. Si esta disposición la enlazamos con la configuración de responsable y encargado habrá que deducir, que el hecho de que estas personas no sigan las instrucciones del responsable (o incluso yendo en contra de estas instrucciones) y actúen de acuerdo con lo establecido en una ley no activará su responsabilidad[731].

4.3.2. El deber de seguridad

a. La formulación del deber de seguridad

Los Estados miembros deben imponer al responsable una obligación consistente en la adopción de medidas técnicas y organizativas adecuadas para proteger los datos (art. 17.1 Directiva 95/46/CE). En concreto, estas medidas deben proteger los datos de la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular, cuando el tratamiento incluya la transmisión de datos dentro de una red. También se indica a modo de cajón de sastre que la protección será contra cualquier otro tratamiento ilícito de datos personales.

El responsable no será el único sujeto obligado a cumplir con esta obligación de seguridad, sino que también corresponderá al encargado del tratamiento (art. 17.3

[730] De nuevo cabe aludir al proceso de elaboración de la Directiva 95/46/CE, ya que al configurarse en un principio esta obligación como una prohibición de divulgación a terceros de los datos, lo que se hizo fue prever una excepción a la misma para que se pudieran comunicar datos cuando así se estableciera en la legislación. Como ejemplo se puso el caso de que fuera necesaria la comunicación de datos para un proceso penal. M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, págs. 160 a 161. En la Ley checa esta obligación de confidencialdiad se establece sin perjuicio de las que establezcan leyes específicas (art. 15.2 Ley checa) y no se aplicará si leyes específicas obligan a proporcionar información (art. 15.3 Ley checa). En la Ley danesa se establece que las personas o empresas que realicen algún trabajo para el responsable o el encargado del tratamiento deberán tratar los datos de acuerdo con las instrucciones del responsable excepto si se establece otra cosa en las leyes o regulaciones (art. 41.1 Ley danesa). Por tanto, se deja abierta la posibilidad de que, en caso de que la ley establezca algo que va en contra de las instrucciones del responsable no deban seguir éstas. Se amplía en esta ley esta salvedad, ya que se añade que las instrucciones que pueda dar el responsable no podrán restringir la libertad de información ni impedir la creación de un producto artístico o literario.

[731] Ver Capítulo II.

Directiva 95/46/CE)[732]. No obstante, el responsable debe asegurarse que este encargado reúne las garantías suficientes para cumplir con estas medidas y después debe velar porque las cumpla (art. 17.2 Directiva 95/46/CE).

Las medidas que deben adoptarse garantizarán un nivel de seguridad apropiado con relación a los riesgos que presente el tratamiento y la naturaleza de los datos a proteger. La adopción de las medidas debe tener en cuenta los conocimientos técnicos existentes -la *lex artis*- y el coste de su aplicación[733]. En consecuencia, esta disposición permite flexibilidad en la determinación de las medidas a adoptar por el responsable. Como indica el TJUE, hay que tener en cuenta que las obligaciones impuestas al responsable no impliquen una carga excesiva, y menciona esta flexibilidad relativa a las medidas de seguridad, como ejemplo de la búsqueda de la proporcionalidad por parte de la Directiva 95/46/CE[734]. En este sentido, se ha planteado si debe atenderse al tamaño de la organización responsable del tratamiento para relajar el nivel de exigencia en la adopción de medidas de seguridad[735].

[732] Algunas leyes asignan expresamente esta obligación de cumplir con las medidas de seguridad al responsable y al encargado del tratamiento (art. 24 Ley eslovena, art. 25.1 Ley letona, art. 30 Ley lituana, art. 13.1 Ley checa). No obstante, la Ley polaca establece que el responsable debe designar un administrador de la seguridad de la información que supervise el cumplimiento de los principios de seguridad, a no ser que el responsable lleve a cabo estas actividades él mismo (art. 36.3 Ley polaca). También como se verá en la legislación española se debe designar para ciertas categorías de datos un responsable de seguridad que se ocupará de que se cumplan las medidas de seguridad (art. 95 RLOPD). Sin embargo, se deja también claro que este responsable de seguridad no supone la exoneración de la responsabilidad que corresponde al responsable o al encargado (art. 95 RLOPD).

[733] En el proceso de elaboración de la Directiva 95/46/CE se incluyó inicialmente el criterio del coste de la aplicación de las medidas para luego eliminarse del texto y finalmente volver a incorporarse en la versión final de la directiva a petición de las delegaciones de Alemania, Dinamarca, Irlanda y Reino Unido. M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, pág. 163. En la Ley húngara se establece que ante la posibilidad de elegir entre diversas soluciones técnicas disponibles para tratar datos debe optarse por la que proporcione el nivel más elevado de protección de datos, excepto si esto conllevara un coste que no fuera razonable para el responsable (sección 7.6 Ley húngara).

[734] Sentencia del TJUE de 7 de mayo de 2009, *College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer*, C-553/07, EU:C:2009:293, apdo. 62.

[735] La Ley eslovena establece que los responsables con menos de cincuenta empleados no deben cumplir con la obligación de documentar los procedimientos y medidas de seguridad y de definir las personas responsables de ficheros y personas que por la naturaleza de su trabajo deben tratar datos (art. 7.4 en relación con art. 25.2 Ley eslovena). Este precepto no se aplica a los siguientes responsables: responsables del sector público, notarios públicos, abogados, detectives, alguaciles, proveedores de servicios de seguridad, trabajadores del sector sanitario privado, proveedores de servicios de salud, y a responsables que mantienen ficheros que contengan categorías especiales de datos y en los que el tratamiento de estos datos forme parte de su actividad. Ver Capítulo IX respecto a esta cuestión en el marco de la reforma de la Directiva 95/46/CE.

La Directiva 95/46/CE parece apuntar a que debiera ser el responsable de tratamiento el que, en función de todos estos aspectos, decidiera las medidas de seguridad pertinentes para conseguir el objeto perseguido, la seguridad de los datos. Así se desprende de la sentencia del TJUE en el asunto *Worten*[736]. No obstante, las legislaciones nacionales, en algunos casos, han optado por establecer medidas concretas a adoptar[737] o han previsto el desarrollo de las mismas en otras normativas[738].

[736] La empresa Worten no había permitido el acceso a los inspectores de trabajo portugueses al sistema de control horario. Esta consulta inmediata se hallaba prevista en el Código de trabajo portugués. Worten afirmaba que permitir este acceso inmediato hubiera supuesto incumplir con las medidas de seguridad previstas en la Directiva 95/46/CE. Entre las preguntas que se plantean en esta cuestión prejudicial estaba la de si el Estado portugués estaba obligado a prever medidas de seguridad necesarias para proteger los datos personales. El TJUE indica que los Estados miembros están obligados a adoptar una disposición de dercho interno que establezca la obligación, por lo que se deduce que no es necesario que la desarrolle. El tribunal entiende que el responsable del tratamiento obligado a cumplir con esta obligación no es el Estado, en este caso, sino la empresa. Concluye, por tanto que el responsable debe asegurar que se cumple con esta obligación, de forma que se asegure que sólo acceda quien esté autorizado a hacerlo: "corresponde a los responsables del tratamiento de datos personales, en virtud del artículo 17, apartado 1, de la Directiva 95/46, adoptar las medidas técnicas y de organización necesarias para garantizar que sólo las personas debidamente autorizadas para acceder a los datos personales de que se trata puedan responder a una solicitud de acceso procedente de un tercero". Sentencia del TJUE de 30 de mayo de 2013, *Worten,* C-342/12, EU:C:2013:355, apdos. 25, 28. También cabe mencionar una sentencia del TEDH, en la que el recurrente alegaba que un hospital público no había protegido su historia clínica, a la que habían accedido personas no autorizadas. Entendía que el motivo era que el Estado finlandés no había establecido las medidas de seguridad concretas que los responsables debían adoptar para asegurar esa protección. La legislación finlandesa en el momento de los hechos, a inicios de los noventa, establecía de forma general la obligación de seguridad. El hospital no tenía limitado el acceso a la historia clínica al personal implicado en la atención de ese paciente. Pese a tener un registro de los accesos a la historia sólo se conservaba un histórico de los cinco últimos. Por tanto, el TEDH consideró que el hospital no cumplía con su obligación de seguridad. Sentencia del TEDH de 17 de octubre de 2008, *I v. Finland*, apdos. 35-49.

[737] La Ley italiana especifica una serie de medidas de seguridad mínimas que deben cumplir todos los responsables. Estas medidas se incluyen en el Anexo B de la ley según establecen los artículos 34 y 35, para el tratamiento a través de medios electrónicos y para el tratamiento sin uso de medios electrónicos respectivamente y está previsto que el gobierno las actualice si lo considera necesario para adaptarlas al progreso de la técnica (art. 36 Ley italiana). Mencionan escuetamente algunas medidas de seguridad: el parágrafo 14 Ley austríaca, el artículo 15 Ley portuguesa, la Sección 7.5 Ley húngara, el artículo 23 Ley luxemburguesa y el artículo 25 Ley estonia.

[738] El RLOPD incluye en su Título VIII las medidas de seguridad que deben adoptar el responsable y el encargado. También establecen la vía del desarrollo reglamentario para incluir las medidas de seguridad: el artículo 39a Ley polaca, el artículo 26.1 Ley letona, el artículo 30.2 Ley lituana, el artículo 9.2 Ley de Liechtenstein, el artículo 13 Ley noruega, el artículo 41.5 Ley danesa, el artículo 23 Ley búlgara. No se detallan medidas de seguridad en las Leyes francesa (aunque para determinadas categorías especiales de datos se establece que la autoridad de control puede fijar medidas detalladas), inglesa (se establece la obligación general en su séptimo principio de protección de datos, en el Anexo 1 de la ley y en las disposiciones interpretativas de la Parte II de este Anexo. Como punto específico a resaltar es que se incluye la obligación para el responsable del tratamiento de adoptar las medidas razonables para asegurar la confianza, la fiabilidad de sus empleados con acceso a los datos personales) e irlandesa.

b. La adaptación al especial contexto tecnológico mediante instrumentos de autorregulación regulada

Si ya en la legislación, en general, existe un problema de falta de adaptación a la realidad social, que se transforma a diario, este problema se acrecienta en el entorno tecnológico que, a cada minuto que pasa, ofrece nuevas posibilidades de interacción que ocasionan nuevos riesgos de vulneración de derechos y nuevas amenazas para los sistemas de información de los responsables. Por lo tanto, en la legislación sobre medidas de seguridad es importante preservar la neutralidad tecnológica, de forma que una medida que parece óptima hoy, no quede desactualizada e inservible para la protección de la información de mañana. Por ello, en las legislaciones nacionales, lo que se hace, es mencionar medidas generales o principios que luego se dejan pendientes de desarrollo en normativas administrativas, que en algunos supuestos quedan en manos de las autoridades de control, como entidades especializadas en el sector[739].

Sin embargo, en un ámbito multidisciplinar, como es éste de las medidas de seguridad, donde se mezcla la protección jurídica de derechos fundamentales, con la regulación de un entorno tecnológico que tiene unas especificidades, es preciso combinar ambos mundos[740]. A esto responde el enfoque adoptado en virtud del riesgo que establece la Directiva 95/46/CE, enfoque que se ha trasladado, en algunos casos a las legislaciones nacionales[741]. Las metodologías de análisis y de gestión de riesgos son propias del ámbito

[739] La Ley luxemburguesa otorga incluso a la autoridad de control la capacidad de poder solicitar una descripción de las medidas y de cualquier cambio que se realice en las mismas (art. 22.1 Ley luxemburguesa). En la Ley letona se obliga a las instituciones gubernamentales estatales y locales a entregar a la autoridad de control cada dos años un informe de auditoría sobre el tratamiento de datos personales, que incluya el análisis de riesgos y un informe sobre las medidas de seguridad aplicadas (art. 26.2 Ley letona). La Ley rumana establece que la autoridad de control desarrollará los requerimientos de seguridad mínimos que deben adoptarse y los actualizará periódicamente (art. 20.2 Ley rumana). Además en casos concretos la autoridad de control podrá decidir que el responsable adopte medidas de seguridad adicionales (art. 20.4 Ley rumana). La Ley islandesa establece que la autoridad de control podrá establecer instrucciones respecto a esta obligación (art. 11 Ley islandesa).

[740] Como ejemplo de ley que sigue un enfoque tecnológico citar la Ley estonia que al establecer la obligación de adopción de medidas de seguridad para proteger los datos estipula tres elementos alrededor de los que gira la adopción de estas medidas: la integridad, la disponibilidad y la confidencialidad de los datos (art. 25 Ley estonia). Estos son algunos de los elementos que tradicionalmente definen la seguridad desde una perspectiva tecnológica.

[741] La Ley checa obliga al responsable y al encargado del tratamiento a desarrollar y documentar las medidas adoptadas para asegurar la protección de los datos de acuerdo con lo que establezca la ley y las normas que la desarrollen y además deberán realizar una evaluación de riesgos (art. 13.2 Ley checa). Respecto al tratamiento automatizado responsable o encargado deberán asegurar que sólo las personas autorizadas acceden a los sistemas, que éstas acceden en virtud de sus permisos, que se establecen los registros necesarios para verificar quien, cuando y porqué se accedió a los datos y para prevenir un acceso

tecnológico[742]. En las mismas se parte de la premisa de que la seguridad absoluta no es un factor alcanzable, sino que deben evaluarse los riesgos a los que está sometida la información y reducirlos al máximo[743]. En este entorno se suele acudir a la estandarización, de forma que se obtienen unos protocolos de actuación que permiten adaptarse mejor al voluble desarrollo de la tecnología.

En la protección de datos se ha adoptado de forma progresiva y natural lo que se conoce como autorregulación regulada[744]. Esta nueva posibilidad de regulación se fundamenta en la cooperación entre la actuación estatal y la autorregulación[745]. Ante el aumento de la complejidad de nuestra sociedad tecnológica causada por diversos factores, como la globalización, el Estado ha tenido que encontrar nuevas formas de regular que permitan abarcar esa complejidad. Para ello, el Estado ha utilizado diferentes instrumentos de autorregulación, que se apoyan, tanto en la elaboración de reglas técnicas por los profesionales expertos en la materia, como en la incorporación de componentes de ética en la conducta de las corporaciones[746].

---

no autorizado a los dispositivos de almacenamiento (art. 13.4 Ley checa). En la Ley islandesa se obliga también a que, tanto el análisis de riesgos, como las medidas de seguridad, se actualicen periódicamente y que el responsable documente la política de seguridad, cómo efectúa el análisis de riesgos y cómo decide sobre las medidas de seguridad a aplicar. La autoridad de control podrá acceder a esta información en cualquier momento (art. 11 Ley islandesa). El responsable deberá realizar auditorías internas al tratamiento de datos para asegurar que se lleva a cabo de acuerdo con la legislación aplicable y que las medidas de seguridad se han aplicado. Estas auditorías deben realizarse periódicamente, como mínimo anualmente y debe obtenerse un informe por escrito que la autoridad de control podrá revisar cuando lo estime conveniente. La autoridad de control podrá emitir instrucciones sobre cómo realizar estas auditorías (art. 12 Ley islandesa).

[742]Las metodologías de evaluación y gestión de riesgos son diversas. Ejemplo de ellas son la ISO 31000 de gestión de riesgos o la ISO/IEC 27005 de gestión de riesgos de seguridad de la información; *Risk IT* de ISACA; OCTAVE (*Operationally Critical Threat, Asset and Vulnerability Evaluation)* de *Carnegie Mellon University Software Engineering Institute* o MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), ésta última elaborada por el Consejo Superior de Administración Electrónica de España.

[743] La seguridad se define como "la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles." Artículo 4.c Reglamento (CE) n 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información, DO L 77 de 13.3.2004.

[744] Sobre este tema, M.M. DARNACULLETA I GARDELLA, *Autorregulación y derecho público: la autorregulación regulada*, Marcial Pons, Madrid, 2005.

[745] M.J. GARCÍA MORALES, "Poderes públicos, autorregulación y protección del consumidor en Internet: a propósito de la regulación del distintivo público de confianza", L. COTINO HUESO (Coord.) VVAA, *Consumidores y usuarios ante las tecnologías*, Tirant lo Blanch, Valencia, 2008, pág. 259.

[746] DARNACULLETA I GARDELLA nos ofrece una enumeración de instrumentos de autorregulación que divide en normativos (códigos de ética y/o de conducta, normas técnicas, códigos y manuales de buenas prácticas, protocolos y procedimientos normalizados de trabajo), declarativos (declaraciones de autorregulación o autocertificación de conformidad a normas, certificados técnicos emitidos por terceros, sellos, etiquetas y marcas) y resolutivos (sanciones disciplinarias, resoluciones arbitrales). M.M.

En el marco de la UE, ya en los años ochenta se optó enseguida por acudir a un sistema de corregulación en el ámbito de la seguridad industrial[747]. Se combinaba la legislación, en forma de directivas, que definía los requisitos esenciales de seguridad de los productos, con la estandarización[748]. De esta forma, se acudía a las organizaciones europeas de normalización[749] para que emitieran los estándares que desarrollaban esos requisitos y que eran voluntarios para los fabricantes. Así se evitaba que las directivas tuvieran que ser muy detalladas y que, por tanto, no permitieran su objetivo que era desarrollar el mercado interior y asegurar la libre circulación de productos. La Directiva 95/46/CE no entraba en el ámbito de esta normativa industrial, por lo que no se aplicó este sistema[750].

Sin embargo, se ha trabajado en la senda de la normalización también en este ámbito de la protección de datos[751]. Fruto de este esfuerzo fueron algunos estándares que elaboró la CEN en el marco del proyecto *Initiative for Privacy Standardisation in Europe* (IPSE), que promovió la Comisión Europea con el fin de facilitar el cumplimiento de la Directiva 95/46/CE a los responsables y encargados del tratamiento que fueran pequeñas y medianas empresas[752]. No obstante, estos estándares estaban más orientados a la gestión

---

DARNACULLETA I GARDELLA, *Autorregulación y derecho público: la autorregulación regulada*, *op. cit.*, págs. 350 a 366.

[747] J.K. WIN, "Technical standards as data protection regulation", S. GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWANGNE, S. NOUWT (Ed.) VVAA, *Reinventing data protection?* Springer, Nehterlands, 2010, págs. 194 a 195. M.M. DARNACULLETA I GARDELLA, *Autorregulación y derecho público: la autorregulación regulada*, *op. cit.*, págs. 114 a 116.

[748] Este sistema se denominó *New approach* (nueva aproximación o nuevo enfoque) y se recogió en la Resolución del Consejo de 7 de mayo de 1985 relativa a una nueva aproximación en materia de armonización y de normalización, DO L 136 de 4.6.1985.

[749] Estas organizaciones son: *European Committee for Standardization* (CEN), *European Committee for Electrotechnical Standardization* (CENELEC) y *European Telecommunications Standards Institute* (ETSI).

[750] J.K. WIN, "Technical standards as data protection regulation", S. GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWANGNE, S. NOUWT (Ed.) VVAA, *Reinventing data protection?* Springer, 2010, pág. 195.

[751] El GA29 ha apoyado la utilización de esta vía. Se pueden citar el Dictamen 1/2002 relativo al informe del CEN/ISS sobre la normalización de la protección de la vida privada en Europa, 10761/02/ES/Final WP 57, 30.5.2002, Grupo de trabajo Artículo 29 sobre la protección de datos y el Dictamen 1/97 sobre las iniciativas canadienses relativas a la normalización en materia de protección de la intimidad, XV/5023/97 final Corr ES WP 2, 29.5.1997, Grupo de trabajo Artículo 29 sobre la protección de datos.

[752] Los documentos son: *CWA 16113 Personal data protection good practices; CWA 15499-1 Personal data protection audit framework, Part 1 Baseline framework; CWA 15499-2 Personal data protection audit framework, Part II Checklists, questionnaires and templates for users of the framework; CWA 1562 Inventory of data protection auditing practices; CWA 15263 Analysis of privacy protection technologies, privacy-enhancing technologies, privacy management systems and identity management systems, the drivers thereof and the need for standardization; CWA 15292 Standard form contract to assist compliance with obligations imposed by article 17 on the Data protection Directive 95/46/EC (and implementation guide).*

que a ser requerimientos técnicos[753]. En el marco de las organizaciones *International Organisation for Standardization* (ISO) y la *International Electrotechnical Commission* (IEC) se adoptó el *Privacy Framework* (ISO/IEC 29100:2011) que proporciona un marco de referencia para la protección de la privacidad[754].

El responsable necesita de herramientas tecnológicas para poder tratar los datos y, en consecuencia, depende de que estas herramientas hagan posible que se puedan proteger los datos. Pero ¿qué sucede si estas herramientas no incluyen estas medidas de protección? ¿Es obligatorio que un programa informático cumpla con las medidas de seguridad establecidas en la normativa de protección de datos? Lo lógico sería entender que sí pero, de nuevo, nos enfrentamos a un mundo globalizado.

Un programador estadounidense puede ser que no tenga en cuenta la normativa de protección de datos europea, pero es que un programador de un Estado de la UE igual tampoco tiene en cuenta las normativas en materia de medidas de seguridad que puedan haberse adoptado en los otros veintisiete países restantes de la UE. Por último, un programador que no adapta su programa a estas normativas no sería perseguible en virtud de un incumplimiento de la normativa de protección de datos, ya que los mecanismos de responsabilidad están configurados para perseguir al responsable. Por eso, en una tendencia expansiva del ámbito de la responsabilidad en algunas leyes nacionales como la alemana se ha querido incluir nuevos sujetos obligados[755].

---

[753] J.K. WIN, "Technical standards as data protection regulation", S. GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWANGNE, S. NOUWT (Ed.) VVAA, *Reinventing data protection?*, *op. cit.*, pág. 202.

[754] ISO/IEC 29100:2011(E), *Joint Technical Committee* ISO/IEC JTC 1, *Information technology, Subcommittee SC 27, IT Security techniques*.

[755] Una peculiaridad de esta norma es la introducción de una definición que se refiere al almacenamiento en soportes y en dispositivos móviles. Con relación a esta definición se crea un nuevo sujeto que es la entidad que decide crear un dispositivo o soporte destinado al tratamiento de datos personales o un procedimiento para tratar datos que funcione en uno de estos dispositivos. Se establece para este sujeto una serie de obligaciones (art. 6c Ley alemana). Principalmente se obliga a este sujeto a informar al afectado de su identidad, dirección, del manual de funcionamiento del dispositivo de forma que se incluya el tipo de datos personales que se tratarán, cómo puede ejercer los derechos de acceso, rectificación, cancelación y oposición tanto en relación a entidades del sector público como privado, y, por último, las medidas que se adoptarán en caso de pérdida o destrucción del dispositivo. El sujeto debe asegurarse de que el afectado pueda ejercer su derecho de acceso de forma gratuita. Los procedimientos de comunicación que inicien el tratamiento de datos en el dispositivo deben ser claramente visibles para el afectado. El artículo 9a Ley alemana además se refiere específicamente a la obligación de realizar auditorías. No obstante, el cumplimiento de esta obligación no parece que dependa de los responsables, ya que no se les cita expresamente. Se refiere de forma neutra a los suministradores de sistemas de tratamiento de datos y programas informáticos, y sujetos que lleven a cabo el tratamiento de datos. Estos sujetos son los que podrán tener expertos independientes que examinen y evalúen su estrategia de protección de datos y los sistemas de información. El procedimiento de auditoría y el de selección de los expertos se regulará en otra

Con este objetivo, también se desarrollaron otros mecanismos directamente relacionados con la tecnología. Así, por ejemplo, ya en la Directiva 1999/5/CE se incorporó la posibilidad de que la Comisión pudiera decidir si los equipos radioeléctricos o los terminales de comunicación debían construirse de forma que incluyeran salvaguardias que garantizaran la protección de datos personales y de la intimidad del usuario y del abonado[756].

En esta línea de incorporar la protección en la tecnología, la Comisión impulsaba, en el 2007, las llamadas *Privacy Enhancing Technologies* o PET, tecnologías que protegían la privacidad[757]. Eran tecnologías que suprimían o reducían los datos personales o evitaban su tratamiento innecesario o indeseado, sin menoscabar la funcionalidad del sistema de información[758]. Una de las acciones que proponía la Comisión para incentivar el uso de estas PET era solicitar a las organizaciones europeas de normalización que evaluaran la aprobación de estándares que incentivaran el desarrollo de las mismas[759].

La concepción de las PET evolucionó hacia lo que se conoció como los principios de protección de datos desde el diseño (*privacy by design)* o protección de datos por defecto (*privacy by default)*[760]. De esta forma, con el *privacy by design* se pasó de añadir una capa de tecnología adicional a la tecnología utilizada, a incluir la protección de datos desde el momento del diseño de la tecnología, para que así se tuviera en cuenta su

---

ley. La ley hace referencia además a los procedimientos automatizados de recuperación de datos, en su artículo 10. Se incluyen en esta disposición obligaciones para los sujetos que estén implicados en la realización de estos procedimientos que pueden implicar la transferencia de datos. Por ejemplo deben asegurar que estos procedimientos puedan ser monitorizados.

[756] Esta previsión se incluía en el artículo 3.3.c) Directiva 1999/5/CE del Parlamento Europeo y del Consejo, de 9 de marzo de 1999, sobre equipos radioeléctricos y equipos terminales de telecomunicación y reconocimiento mutuo de su conformidad, DO L 091, 7.4.1999, pág. 10.

[757] Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET), COM(2007) 228 final, Bruselas, 2.5.2007.

[758] *Ibídem*, pág. 3-4. Se indicaban como ejemplos de estas tecnologías las que convertían en anónimos los datos tras un lapso de tiempo, el cifrado, los mecanismos de bloqueo de cookies o la Plataforma de Preferencias de Privacidad (P3P).

[759] *Ibídem*, pág. 7.

[760] Este término de *privacy by design* fue desarrollado por CAVOUKIAN, la Comisionada de Información y Privacidad de Ontario, Canadá, en los años noventa. A. CAVOUKIAN, *Privacy by design… Take the challenge*, Information and Privacy Commissioner of Ontario, Ontario, 2009, pág. 3. El Considerando 46 Directiva 95/46/CE ya se refiere a que la adopción de las medidas de seguridad debe realizarse "tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos, sobre todo con todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado".

protección antes de su desarrollo[761]. La protección de datos por defecto tenía como objetivo cambiar la práctica de los desarrolladores o fabricantes, de configurar los programas y los equipos por defecto sin medidas de seguridad activadas, de forma que los responsables debían activarlas. Se pretendía que estos programas o equipos se distribuyeran con estas medidas de seguridad activadas por defecto.

La importancia de tener en cuenta estos enfoques derivó en que la Comisión, a inicios de 2015, instó un mandato a la CEN para que iniciara un proceso de estandarización, para incorporar la *privacy by design* en los procesos de fabricación y desarrollo de equipos y programas informáticos, y proteger así la privacidad y la protección de datos, en el marco de la Directiva 95/46/CE y la política de seguridad industrial[762]. Por tanto, finalmente, adoptó la acción que proponía en el 2007 en la línea de la corregulación adoptada para el sector industrial. Como indicaba la Comisión en este mandato, las leyes de protección de datos son tecnológicamente neutras y los estándares son útiles para desarrollar estos instrumentos legales. Estos estándares servirán para que los fabricantes y proveedores de servicios apliquen el enfoque de *Privacy by design*, de forma que adopten en sus procesos de diseño y desarrollo, sistemas de gestión que aseguren que se tendrán en cuenta la protección de datos y la privacidad[763].

Otra forma de incentivar la mejora de la protección incorporada en la tecnología es la certificación de productos informáticos o procedimientos que han establecido algunas leyes nacionales, como la alemana o la francesa[764]. La Ley francesa dispone que la autoridad de control francesa pueda otorgar un sello a productos y procedimientos

[761] *Privacy and data protection by design-from policy to engineering, European Union Agency for Network and Information Security (ENISA), December 2014*, pág. 5.
[762] *Commission implemeting Decision of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy, COM(2015) 102 final, Brussels, 20.1.2015.*
[763] *Ibídem (Annex I)*, págs. 3 a 4.
[764] También la Ley de Liechtenstein establece un procedimiento de certificación para productos, sistemas, procedimientos y organización (art. 14a Ley de Liechtenstein). De esta forma aquellos fabricantes de programas o sistemas para tratar datos o aquellas personas del sector público o privado que traten datos personales podrán certificar los elementos mencionados acudiendo a una organización que los evalúe y reconozca. El gobierno por ordenanza elaborará las reglas para la acreditación de los procedimientos de certificación y la introducción de una etiqueta de calidad de protección de datos. Para ello, se establece que el gobierno deberá tener en cuenta la legislación internacional y los standards técnicos reconocidos internacionalmente.

tendentes a la protección de las personas con relación a los tratamientos de datos personales, tras revisar que son conformes a la ley (art. 11.3.c Ley francesa[765]). También se puede acudir a una persona independiente calificada para realizar la evaluación. El coste de la evaluación lo asumirá la empresa que solicita la certificación. Sin embargo, hay que decir que son muy pocos los sellos otorgados[766].

La Ley alemana incluye esta posibilidad de auditar programas informáticos y sistemas de información aunque está pendiente de desarrollo (art. 9a Ley alemana). También, en Alemania se puede mencionar la instauración, ya en el año 1997, de un sistema de auditoría de los servicios de medios de comunicación, con el fin de comprobar la protección de datos por expertos independientes y acreditados[767].

---

[765] El artículo 11.3.c) Ley francesa se modificó en el año 2009 y se reproduce a continuación: "*Elle délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, après qu'elles les a reconnus conformes aux dispositions de la présente loi ; dans le cadre de l'instruction préalable à la délivrance du label par la commission, le président peut, lorsque la complexité du produit ou de la procédure le justifie, recourir à toute personne indépendante qualifiée pour procéder à leur évaluation. Le coût de cette évaluation est pris en charge par l'entreprise qui demande le label*". Esta disposición se desarrolló mediante la modificación del artículo 69 del reglamento de régimen interior de la *Commission Nationales de l'Informatique et des Libertés-CNIL*. En este desarrollo se reguló el procedimiento para otorgar los sellos. Las organizaciones profesionales o instituciones que agrupen a responsables del tratamiento podrán solicitar a la CNIL que cree un sello para un determinado producto o un procedimiento. Si el presidente de la CNIL estima conveniente que se cree el sello se elabora un marco de referencia en el que se precisarán las particularidades de la evaluación a realizar. *Délibération no 2011-249 du 8 septembre 2011 portant modification de l'article 69 du règlement, intérieur de la Commission nationale de l'informatique et des libertés et insérant un chapitre IV bis intitulé « Procédure de labellisation », Commission nationale de l'informatique et des libertés, Journal Officiel de la République Française, 22 septembre 2011*: http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=20110922&numTexte=81&pageDebut=&pageFin=, (consulta: 12.8.2014). Los marcos de referencia aprobados hasta ahora son únicamente dos: el que está referido a procedimientos de auditoría que persiguen la protección de datos de carácter personal: ver *Délibération no 2011-316 du 6 octobre 2011 portant adoption d'un référentiel pour la délivrance de labels en matière de procédure d'audit tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, Commission nationale de l'informatique et des libertés, Journal Officiel de la République Française, 3 novembre 2011*, http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=20111103&numTexte=63&pageDebut=&pageFin=, (consulta: 12.8.2014) y el que se refiere a módulos de formación en materia de protección de datos, ver *Délibération no 2011-315 du 6 octobre 2011 portant adoption d'un référentiel pour la délivrance de labels en matière de formation tendant à la protection des personnes à l'égard du traitement des données à caractère personnel Commission nationale de l'informatique et des libertés, Journal Officiel de la République Française, 3 novembre 2011*, http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=20111103&numTexte=62&pageDebut=&pageFin= (consulta: 12.8.2014).

[766] Se han otorgado 11 sellos a procedimientos de auditoría: http://www.cnil.fr/linstitution/labels-cnil/procedures-daudit/accessible/non/ (consulta: 12.8.2014) y 21 sellos a módulos formativos: http://www.cnil.fr/linstitution/labels-cnil/formations/accessible/non/, (consulta: 12.8.2014).

[767] Sobre este sistema ver: M.J. GARCÍA MORALES, "La regulación de los servicios multimedia en Alemania", *Autonomies*, núm. 25, 1999, págs. 63 a 64 y M.J. GARCÍA MORALES, "Poderes públicos, autorregulación y protección del consumidor en Internet: a propósito de la regulación del distintivo público de confianza", L. COTINO HUESO (Coord.) VVAA, *Consumidores y usuarios ante las tecnologías, op. cit.*, págs. 259 a 261.

Asimismo, en Alemania, pero a nivel estatal, la autoridad de control del *Land* de *Schleswig-Holstein* ha establecido un procedimiento de certificación de productos informáticos en el ámbito de sus competencias[768]. Esta experiencia ha servido para que esta autoridad haya impulsado junto con otras autoridades, entre las que figuraba la extinta Agencia de Protección de Datos de la Comunidad de Madrid, la creación del sello *European Privacy Seal* o "Europrise"[769]. Este sello se otorga a productos de *software* o servicios web y certifica que son compatibles con la normativa europea de protección de datos. Este proyecto, que fue financiado por la Comisión Europea, se inició por algunas autoridades de control[770]. Posteriormente, se creó una sociedad que es la que otorga los sellos, pero la evaluación de los productos y servicios la realizan expertos acreditados por esta sociedad, que la llevan a cabo mediante unos criterios homogéneos adoptados en virtud de la normativa europea[771].

La Ley húngara ha introducido la posibilidad de que los responsables soliciten a la autoridad de control la realización de una auditoría de los tratamientos de datos, de forma que se asegure un elevado nivel de cumplimiento, especialmente en materia de seguridad[772]. Con el fin de que el responsable pueda publicitar que ha realizado esta

[768] La autoridad de control del Estado de Schleswig-Holstein en Alemania (*Unabhängiges Landeszentrum für Datenschutz-ULD* del *Land de Schleswig-Holstein)* ha desarrollado este procedimiento en virtud de lo establecido en el &43 *State data protection Act Schleswig-Holstein 9 February 2000 GS Sch.-H. II, GI.Nr.204-4*, https://www.datenschutzzentrum.de/material/recht/ldsg-eng.htm (fecha consulta: 12.8.2014).

[769] El proyecto también recibió el apoyo de la autoridad de control francesa CNIL. Sobre esta iniciativa ver J. VIGURÍ CORDERO, J., "Los mecanismos de certificación (códigos de conducta, sellos y marcas)", A. RALLO LOMBARTE, R. GARCÍA MAHAMUT (Ed.), VVAA, *Hacia un nuevo derecho europeo de protección de datos. Towards a new European data protection regime*, *op. cit*., págs. 929 a 933.

[770] La sociedad que ahora ha asumido la gestión de esta certificación (*EuroPriSe GmbH*) ha nombrado un Consejo asesor de la autoridad de certificación, entre cuyos miembros están el Dr. Thilo Weichert, director de la autoridad de control mencionada del *Schleswig-Holstein*, Alemania, Dr. John Borking, ex director de la autoridad de control de los Países Bajos o Peter Schaar, que fue director de la autoridad de control federal alemana y estuvo también al frente del GA29. TRONCOSO REIGADA, director de la Agencia de Protección de Datos de la Comunidad de Madrid e impulsor de esta iniciativa entendía que la opción de este sistema en el que los que realizaban la evaluación de los productos o servicios eran expertos acreditados era mejor que optar porque fueran las mismas autoridades de control las que llevaran a cabo la evaluación. A. TRONCOSO REIGADA, *La protección de datos personales. En busca del equilibrio*, *op. cit.*, págs. 257 a 258.

[771] Los sellos otorgados se pueden consultar en https://www.european-privacy-seal.eu/EPS-en/Awarded-seals.

[772] La Ley húngara establece en su Sección 69, que entró en vigor el 1 de enero de 2013, esta posibilidad. Se paga una tasa y el resultado del servicio es un informe de auditoría que también puede contener recomendaciones. Se indica que, el hecho de realizar la auditoría, no excluye que la autoridad de control ejerza otras competencias que le proporciona la ley, lo que parece evitar que se utilice la auditoría como mecanismo de protección ante la amenaza de posibles actuaciones de la autoridad contra el responsable en caso de vulneración. Estas auditorías pueden implicar conflictos y tensiones, y exigen de gran rigor y

auditoría podrá publicar el informe que le proporcione la autoridad, de forma voluntaria. Por último, quiero mencionar los premios que organiza la ACPD desde el año 2013 a aplicaciones informáticas que apliquen el enfoque de *privacy by design*[773]. Esta iniciativa se incardina en lo que se ha venido a llamar el modelo catalán de protección de datos, que persigue un enfoque preventivo, mediante la promoción de mecanismos que ayuden a los responsables y a los encargados a gestionar correctamente los datos para evitar la vulneración de la normativa[774].

5. OBLIGACIONES RELATIVAS A LA FASE DE SALIDA DE DATOS

5.1. La comunicación de datos

Al igual que la recogida de datos, la comunicación de datos es una operación más incluida en la definición de tratamiento de datos personales. Aunque más bien hay que decir que es un grupo de operaciones, ya que, en el concepto, se incluyen: la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos y también se mencionan separadamente el cotejo o interconexión (art. 2.b Directiva 95/46/CE). Por tanto, la comunicación se entiende de forma amplia y no precisa la transmisión material de los datos sino que basta para considerarse una comunicación que se acceda a los datos, aunque estos no se muevan de su ubicación (por ejemplo, un simple acceso en remoto al servidor del responsable).

Esta operación adquiere una cierta relevancia en la regulación de algunas leyes nacionales que la han regulado de forma autónoma[775]. La razón de esta especial atención es, sin duda, el elevado riesgo que suponen para el control y la protección de los datos personales. Hay que decir, como peculiaridad, que las operaciones de cotejo e

---

coherencia para evitar respuestas diferentes después en la actuación de la autoridad, en caso de producirse una acción de investigación o de sanción, en virtud de la normativa.

[773] Se puede encontrar información sobre el *Premi protecció de dades en el disseny* en http://www.apd.cat/ca/contingut.php?cont_id=630&cat_id=712.

[774] Respecto a este modelo catalán de protección de datos, hay que indicar que incluso la Ley catalana establece que la ACPD impulse la evaluación de impacto (art. 5.c Ley catalana), mecanismo que veremos se incorpora en el proyecto de Reglamento General de Protección de Datos que sustituirá a la Directiva 95/46/CE. E. MITJANS PERELLÓ, "El modelo de protección de datos de la Ley 32/2010, de 1 de octubre de 2010, de la Autoridad Catalana de Protección de Datos", *Comunicaciones en propiedad industrial y derecho de la competencia*, nº 63, 2011, págs. 17 a 18.

[775] Se incluyen regulaciones específicas sobre la comunicación de datos en: artículos 11, 21 y 27 LOPD, artículo 23 Ley italiana, artículo 1.1 Ley irlandesa, artículo 11 Ley estonia, artículo 22 Ley eslovena, artículo 6 Ley lituana, artículos 3.1.h) y 23 ley de Liechtenstein.

interconexión se configuran en algunas leyes nacionales, tanto como una comunicación, cuando se realizan entre ficheros de diferentes responsables, como transmisiones en el marco del mismo responsable. Al respecto, la Ley portuguesa ha desarrollado una regulación específica sobre la concreta operación de interconexión [776] y la Ley chipriota sobre la operación de combinación[777].

Sin embargo, la Directiva 95/46/CE, pese al protagonismo que la comunicación tiene en la definición de tratamiento, no establece una regulación independiente para ella, sino que le aplica la regulación general. No obstante, la comunicación de datos sirve para definir el alcance de algunas obligaciones y, para ello, se ayuda de dos figuras que se definen en la Directiva 95/46/CE: el tercero y el destinatario.

5.1.1. El tercero

El concepto de tercero se incluyó en la Propuesta de Directiva de 1992, a raíz de la enmienda 134ª propuesta por el Parlamento Europeo que se inspiró en la Ley federal alemana de 1990[778]. La Comisión entendió que debía utilizarse para delimitar la figura del cesionario o quien recibe la comunicación de datos[779]. Para ello, se extrajeron de la definición a todas las personas que se pudieran conectar con el responsable: "las personas físicas o jurídicas, con excepción del interesado, del responsable del tratamiento y de las

[776] Así, la Ley portuguesa ha definido lo que considera interconexión de datos, de forma que es la posibilidad de cotejar datos de un fichero con los datos de otro fichero que mantiene otro responsable o que mantenga el mismo responsable para otras finalidades (art. 3.i Ley portuguesa). Por tanto, si un mismo responsable quiere realizar esta interconexión entre varios ficheros deberá aplicar la regulación específica que recoge esta ley. La Ley portuguesa regula esta interconexión de datos de forma específica en su artículo 9, de forma que permite que se lleve a cabo si así está previsto en una disposición legal o si lo autoriza la autoridad de control. La solicitud de autorización la deberán remitir el responsable o responsables. De todas formas, se añade que la interconexión sólo podrá realizarse si es necesario para la persecución de las finalidades legales o estatutarias y de los intereses legítimos del responsable, siempre que no impliquen la discriminación o la reducción de los derechos fundamentales y libertades de los interesados, y se apliquen las debidas medidas de seguridad.

[777] La "combinación" se define en la Ley chipriota como una forma de tratamiento que implica la conexión de datos de un fichero con otro fichero que mantiene otro responsable y otros responsables o que mantiene el mismo responsable pero para diferentes finalidades (art. 2 Ley chipriota). La combinación además de tener que cumplir alguno de los supuestos de legitimación, debe notificarse a la autoridad de control. Además se exige la autorización previa de la autoridad de control para poder llevar a cabo la combinación si al menos uno de los ficheros contiene datos sensibles o si de la combinación resulta la comunicación de datos sensibles o si para llevar a cabo la combinación se usará un solo número de identificación (art. 8 Ley chipriota).

[778] M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, pág. 82.

[779] *Ibídem.*

personas autorizadas para tratar los datos bajo su autoridad directa o por su cuenta" (art. 2.f) Propuesta de Directiva de 1992).

En la versión definitiva se completó el elemento subjetivo de la figura para asimilarlo a la del responsable y se hizo referencia al encargado: "tercero: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento (art. 2.f) Directiva 95/46/CE).

Se confirmó, no obstante, que la utilidad del concepto era incorporar a aquellos sujetos que estuvieran fuera del círculo de influencia del responsable. De esta forma, se asimila al concepto de tercero del derecho civil, como un sujeto que no es parte de una relación jurídica determinada, normalmente la que existirá entre el responsable del tratamiento y el interesado[780].

Hay que tener en cuenta que la regulación contenida en la Directiva 95/46/CE se proyecta sobre un supuesto de hecho. Este supuesto de hecho es el ciclo de vida del tratamiento del dato personal en el ámbito de una organización, del responsable del tratamiento. Desde que este responsable recoge el dato de carácter personal hasta que lo expulsa de su radio de acción debe cumplir con lo establecido para cada una de estas fases por la directiva. Pero ¿hasta dónde llega el radio de acción y, por tanto, hasta donde llega la responsabilidad en este circuito lógico del tratamiento de datos?

El tercero ayuda a delimitar este alcance, de forma que se utilizará para establecer que el responsable tiene la obligación de evaluar la legitimación que tiene ese tercero para recibir los datos, en algunos de los supuestos que habilitan el tratamiento de datos[781]. El

[780] En la legislación española se define tercero como "la persona física o jurídica, pública o privada y órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento. Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados" (art. 5.1.r) RLOP). Por tanto, se quiere incluir a cualquiera externo a la relación entre responsable e interesado.

[781] De esta forma, se utiliza este término para establecer la legitimación para tratar datos personales en los siguientes supuestos: cuando sea necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al tercero a quien se comuniquen datos (art. 7.e) Directiva 95/46/CE) y cuando sea necesario para la satisfacción del interés legítimo perseguido por el tercero o

responsable debe valorar si el tercero tiene legitimación para tratar los datos para poder comunicárselos, ya que la comunicación es un tratamiento sobre el que el responsable ejerce su capacidad de decisión.

También comporta una obligación para el responsable la notificación a los terceros a quienes haya comunicado datos de toda rectificación, supresión o bloqueo efectuado de los datos de un interesado en virtud del ejercicio de su derecho de acceso (art. 12.c Directiva 95/46/CE). Estas obligaciones reflejan la posición de garante que la Directiva 95/45/CE otorga al responsable que debe velar, no sólo porque el tratamiento que realiza él mismo es acorde con la normativa, sino que también el tratamiento que realizan los terceros a quienes haya comunicado datos respeta esta normativa.

El especial riesgo de pérdida de control que tiene la comunicación para el interesado se ilustra con la regulación del derecho de oposición, en la que se establece que el responsable deberá informar al interesado, antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección (art. 14.b) Directiva 95/46/CE). Además debe ofrecerse al interesado el derecho a oponerse, sin gastos, a esta comunicación o utilización de los datos. Este peligro implica que también se establezca la comunicación de datos a un tercero como límite temporal al cumplimiento de la obligación de informar al interesado cuando los datos no se recaban directamente del mismo (art. 11 Directiva 95/46/CE)[782].

Otro supuesto en que aparece el término tercero es para limitar la comunicación de datos sin consentimiento de los interesados, en caso de tratamientos de categorías especiales de datos[783]. Asimismo, en el ámbito de las transferencias a países terceros, se

---

terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al artículo 1.1 Directiva 95/46/CE (art. 7.f) Directiva 95/46/CE).

[782] De esta forma se indica que, en caso de que se piense comunicar datos a un tercero deberá proporcionarse la información que se detalla en el artículo como máximo en el momento de la primera comunicación de datos, salvo si el interesado ya hubiera sido informado de estos aspectos (art. 11.1 Directiva 95/46/CE). Además también se utiliza para excepcionar esta obligación de información cuando la comunicación de los datos a un tercero estuviera expresamente prescrita por ley (art. 11.2 Directiva 95/46/CE).

[783] En el artículo 8.2.d) Directiva 95/46/CE se estipula como excepción a la prohibición de tratar datos de categorías especiales de datos, que el tratamiento se efectúe en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por

incluye como supuesto que permite la transferencia a un país tercero que no garantice un nivel de protección adecuado, el hecho de que la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero (art. 26.1.c) Directiva 95/46/CE).

Por tanto, de la utilización que la Directiva 95/46/CE realiza del término tercero se puede extraer que supone el cumplimiento de obligaciones y límites al tratamiento respecto a las comunicaciones de datos a estos terceros. También se utiliza para ilustrar algún supuesto en el que se incluye un sujeto (el tercero) que es ajeno a la relación jurídica, como sucede en este último supuesto referido a las transferencias internacionales pero que, en definitiva, supondrá también una comunicación de datos.

El GA29 indica que también se podrán calificar de terceros a los sujetos que estén dentro del círculo de poder del responsable del tratamiento, cuando "salgan" de este círculo. Es decir si, por ejemplo, un empleado del responsable del tratamiento tiene conocimiento en el ámbito de su trabajo de unos datos a los que no tenía autorizado el acceso. En este caso, el empleado se consideraría tercero respecto del empleador[784].

Del análisis de la utilización del término "tercero" en la Directiva 95/46/CE se concluye que la regulación que esta norma establece para supuestos de comunicación de datos se refiere únicamente a cuando los datos se proporcionan a un tercero. Pero entonces ¿cuál es la finalidad de la definición de destinatario?

5.1.2. El destinatario

Además de la noción de tercero, se incluyó en la Directiva 95/46/CE otro concepto, el de "destinatario", con el fin de establecer garantías adicionales en el caso de que la operación que se llevara a cabo fuera la comunicación de datos, operación que

razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados. Por lo tanto, se trata de un límite en el tratamiento de datos especiales que se establece en este supuesto.

[784] Como ejemplos cita el GA29 que se considerará tercero a la persona que trabaja en otra empresa, aunque ésta forme parte del mismo grupo empresarial pero no será tercero una sucursal bancaria sometida a la autoridad de la oficina principal ni es tercero un agente de seguros, en relación a la compañía de seguros. En este sentido, entiendo que el agente de seguros debe considerarse un encargado del tratamiento y, por tanto, no encaja efectivamente en la definición de tercero. Dictamen 1/2010 del Grupo del Artículo 29, *op. cit.*, pág. 35.

debido a esta pérdida del control al salir del círculo de poder del responsable, conlleva riesgos adicionales.

El destinatario se define como "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios" (art. 2.g) Directiva 95/46/CE). Esta definición, al referirse al tercero, debe ponerse en relación con ésta, lo que nos indica que todos los sujetos, estén bajo el ámbito de influencia del responsable o no, serán destinatario a los efectos de la regulación de la Directiva 95/46/CE, con la única excepción de la autoridad que reciba datos en el marco de una investigación.

Si acudimos al proceso legislativo de la Directiva 95/46/CE, comprobamos que este concepto se incluyó en la versión final directamente, a iniciativa de la delegación francesa y de la Comisión, que propusieron deslindar esta noción de la de tercero[785]. La explicación para hacerlo es "que es útil para garantizar la transparencia de los tratamientos con respecto a las personas afectadas"[786]. Por tanto, la única finalidad por la que se introduce este concepto de destinatario en la Directiva 95/46/CE es para incrementar la transparencia en el tratamiento de datos de cara al interesado.

En el texto de la Directiva 95/46/CE el término aparece trece veces: en la definición y en los artículos 10.c) y 11.c), ambos relativos a la información al interesado, 12.a) relativo al derecho de acceso y 18.2, sobre la notificación a la autoridad de control. En todos ellos, no se pretende regular la comunicación de datos sino que el interesado conozca a quien se proporcionarán los datos[787].

---

[785] M. HEREDERO HIGUERAS, *La Directiva comunitaria de protección de los datos de carácter personal (…), op. cit.*, pág. 82.

[786] Posición común (CE) nº1/95 adoptada por el Consejo el 20.2.1995 con vistas a la adopción de la Directiva 95/…/CE del Parlamento Europeo y del Consejo, de …, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO C 93 de 13.4.1995, apdo. 2.i.

[787] En el marco del artículo 10 Directiva 95/46/CE se ofrece a los Estados miembros la posibilidad de que incluyan como información no esencial que puede proporcionarse al interesado, si se han obtenido los datos directamente de éste, "los destinatarios o las categorías de destinatarios de los datos". Del mismo modo se incluye esta posibilidad en el artículo 11 Directiva 95/46/CE cuando los datos no hayan sido recabados del propio interesado. En el artículo 12 Directiva 95/46/CE que regula el derecho de acceso, ya no ofrecido como una posibilidad a los Estados miembros, sino como parte de la información que el responsable del

La inclusión de estas definiciones de tercero y destinatario en la Directiva 95/46/CE ha provocado que en la transposición de la directiva, algunas leyes nacionales hayan reflejado de forma algo confusa esta regulación[788]. De hecho, en algunas leyes nacionales se utiliza el término destinatario en el ámbito del establecimiento de una concreta regulación respecto a la comunicación de datos[789].

5.2. El encargo del tratamiento

La Comisión Europea ha considerado que las divergencias existentes respecto al encargado del tratamiento en las legislaciones nacionales van en contra de la libre

tratamiento debe proporcionar al interesado que ejerza este derecho también se incluye la información relativa a "los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos". En el artículo 18.2 Directiva 95/46/CE y, para el caso de que los Estados miembros optaran por disponer la simplificación o la omisión de la obligación de notificación de los tratamientos de datos a la autoridad de control, lo hagan respecto a categorías de tratamientos que no afecten a los derechos y libertades de los interesados habida cuenta de los datos a que se refiere el tratamiento. Para ello, se exige que los Estados miembros precisen los fines de los tratamientos, los datos o categorías de datos tratados, la categoría o categorías de los interesados, los destinatarios o categorías de destinatarios a los que se comuniquen los datos y el período de conservación de los datos.

[788] La Ley irlandesa especifica, para evitar confusiones, que no se entenderá que hay comunicación cuando se faciliten los datos de forma directa o indirecta por el responsable o por el encargado del tratamiento a sus empleados o agentes para que lleven a cabo sus tareas (art. 1.1 Ley irlandesa). La Ley polaca no incluye definición de tercero, sino sólo de destinatario pero ésta encaja con la definición de la Directiva 95/46/CE de tercero (art. 7.6 Ley polaca). La Ley croata incluye una regulación específica relativa a la comunicación de datos a terceros, pero estos terceros se denominan usuarios (*users*). Estos usuarios se definen como la persona física o jurídica, estado u otro órgano a quien los datos se le pueden comunicar con la finalidad de llevar a cabo actividades habituales dentro del ámbito de su competencia, tal como se define en la ley (art. 2.5 Ley croata). De esta forma, no coincide esta definición ni con la de tercero ni con la de destinatario en la Directiva 95/46/CE. La ley autoriza expresamente al responsable a comunicar datos a estos usuarios pero para ello, el usuario debe solicitárselo por escrito al responsable y debe ser necesario para llevar a cabo tareas incluidas en la actividad del usuario según se defina en la ley (art. 11 Ley croata). En esta solicitud se debe incluir el fin y la base legal para la utilización de los datos y el tipo de datos solicitados. Además la ley exige que se cumpla con las previsiones dedicadas a la legitimación del tratamiento de datos y al principio de calidad y que el responsable mantenga un registro de la información proporcionada, a quién se ha proporcionado y la finalidad.

[789] En la legislación española se asimila al destinatario con el cesionario y se le define como "la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos. Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados" (art. 5.1.h) RLOPD). Esta figura tiene un papel en la regulación de la comunicación, de forma que se utiliza para algunos aspectos en los que la Directiva 95/46/CE atribuía el papel al tercero.La Ley húngara establece una regulación específica para la comunicación de datos en su Sección 9, dentro del apartado 8 de la ley, que se titula "restricciones al tratamiento de datos" y que incluye sólo esta sección. Por tanto, se subraya el riesgo que para el derecho de protección de datos suponen las comunicaciones y se impone el peso de las obligaciones, en estos casos, al responsable que transmite los datos. El destinatario no se define en la Ley húngara tal como se hace en la Directiva 95/46/CE, sólo se indica que es quien recibe los datos del responsable.

circulación de datos en el mercado interior[790]. En algunas de estas leyes ni siquiera se incluye esta figura sino que se reconducen a otras como la del tercero[791].

La Directiva 95/46/CE establece que si el responsable debe encargar un tratamiento a un tercero debe elegir un encargado del tratamiento que reúna garantías suficientes para cumplir con las medidas de seguridad preceptivas[792] y además deberá asegurarse de que cumple efectivamente con estas medidas (art. 17.2 Directiva 95/46/CE). También debe suscribir un contrato con el encargado (art. 17.3 Directiva 95/46/CE).

En lo que respecta a las obligaciones que se generan para el encargado del tratamiento en la Directiva 95/46/CE, serían tres asignadas expresamente: tratar los datos cuando se lo encargue el responsable del tratamiento o un imperativo legal y de acuerdo a las instrucciones del responsable, cumplir con las medidas de seguridad que establezca la legislación nacional aplicable y suscribir un contrato con el responsable (arts. 16 y 17 Directiva 95/46/CE)[793].

---

[790] *Commission Staff Working Paper, Impact assessment accompanying the document Regulation of the European Parliament […], op. cit., Annex 2,* págs. 16 a 19.

[791] En el caso de los encargados del tratamiento, la Ley alemana no se refiere a la empresa contratante como responsable, sino como principal (en la traducción al inglés *principal*). Entiendo que esto se debe a que establece este mismo artículo que el encargo puede realizarlo la autoridad de control, en el caso del sector público, entidad que no encajaría en el papel de responsable. Tampoco se refiere este artículo al encargado del tratamiento con este término sino con el de agente (*agent*) ya que no se ha establecido en la ley una definición de encargado del tratamiento (art. 11 Ley alemana). La Ley de Liechtenstein no contempla la definición del encargado del tratamiento, de forma que cuando se refiere a esta regulación, denomina a este encargado como tercero y no se hace tampoco referencia al responsable del fichero sino que se indica que el tratamiento se podrá encargar a un tercero y la parte mandante se asegurará de que el tratamiento no se efectúe si esta parte no pudiera efectuarlo y que el tratamiento no esté prohibido por una obligación legal o contractual de confidencialidad (art. 19.1 Ley de Liechtenstein).

[792] La Ley finlandesa establece una somera regulación de esta figura del encargado del tratamiento que incide en este requisito relativo a las garantías que debe reunir el encargado (art. 32.2 Ley finlandesa). La Ley islandesa, en su regulación del encargado del tratamiento, establece la obligación del responsable de verificar que el encargado es capaz de cumplir con las medidas de seguridad y para ello se incluye la capacidad del responsable de realizar las auditorías internas que esta ley prevé (en su art. 12). La legislación española también contempla esta obligación del responsable de velar porque el encargado reúna las garantías para cumplir lo establecido en el RLOPD (art. 20.2 RLOPD), ver Capítulo VI. En algunas leyes además se especifican requisitos adicionales que debe cumplir el encargado del tratamiento y que se orientan a estas garantías previas. En la Ley húngara se establece lo que parece una incompatibilidad para ser encargado si el sujeto tiene un interés comercial en los datos (sección 10 Ley húngara). La Ley eslovena dispone que el encargado del tratamiento debe tener una actividad registrada que le habilite para llevar a cabo las tareas encomendadas por el responsable y debe asegurar el cumplimiento de las medidas de seguridad (art. 11.1 Ley eslovena).

[793] Como importantes divergencias en una ley nacional, destacar que en la Ley de Liechtenstein no se hace referencia a que el tercero (el encargado del tratamiento) deba actuar siguiendo las instrucciones del mandante (el responsable). Además debe resaltarse que la regulación del encargado se contempla únicamente en la parte de la norma dedicada al sector privado.

En virtud de la ubicación sistemática de la figura del encargo del tratamiento (Sección VIII Directiva 95/46/CE, dedicada a la confidencialidad y seguridad del tratamiento) cabe plantearse si el encargado del tratamiento estaría eximido de cumplir con las demás obligaciones establecidas en la Directiva 95/46/CE (calidad, atender el ejercicio de los derechos, deber de notificar, etc.). Si acudimos a las obligaciones, de entre las que se adjudicaban expresamente al responsable estaba la relativa a los principios de calidad que indica: "corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1" (art. 6.2 Directiva 95/46/CE). El hecho de indicar que debe "garantizar" el cumplimiento y no que debe cumplir presupone que podrá ser otro el que deba cumplir por cuenta del responsable.

Respecto al resto de las obligaciones, asignadas expresa o implícitamente al responsable del tratamiento, cabría inicialmente pensar que debe cumplirlas de forma exclusiva el responsable, en especial la relativa a los supuestos que habilitan el tratamiento[794]. Sin embargo, es evidente que, de igual modo que debe entenderse que el encargado actúa bajo el manto de la legitimación que ostenta el responsable, debe actuar también como actuaría el responsable y debe respetar, en consecuencia, los mismos principios que el responsable, aunque limitado a sus instrucciones. No tendría sentido que el encargado no debiera respetar los principios de calidad o las limitaciones del tratamiento de categorías sensibles.

No obstante, el encargado deberá abstenerse de llevar a cabo cualquier aspecto de estas obligaciones que implique adoptar una decisión sobre los fines o los medios esenciales del tratamiento. En esos casos deberá recurrir al responsable para que sea quien tome esta decisión. Ahora bien, no parece que esto impida que el responsable del

[794] Hay que decir que la Ley checa establece que las obligaciones de su artículo 5 se aplican también al encargado. Este artículo 5 es el que establece los principios de calidad y los supuestos de legitimación del tratamiento. Esta regulación es excepcional pero es un ejemplo de esta cuestión, ya que se asigna al encargado obligaciones que son propias del responsable (art. 7 Ley checa). Hay que entender que el hecho de que el encargado deba cumplir con estas obligaciones lo que implica es que lo hace por cuenta del responsable y, por tanto, no puede desviarse del supuesto que legitimó el tratamiento ni puede incumplir los principios de calidad. La Ley de Liechtenstein indica que el tercero (así se denomina al encargado del tratamiento en esta ley) estará sometido a las mismas obligaciones y deberá atenerse a la misma justificación lícita que la parte mandante (art. 19.2 Ley de Liechtenstein). La Ley islandesa indica que en el contrato además de estipularse que el encargado sólo debe actuar según las instrucciones del responsable también debe indicar que el encargado debe cumplir con las obligaciones que establece la Ley islandesa (art. 13 Ley islandesa).

tratamiento pueda encomendar al encargado del tratamiento, como parte de su mandato, que cumpla con algunas de estas obligaciones que impliquen decisiones siempre que sea bajo las instrucciones previas del responsable. De esta forma, es lógico que si, por ejemplo, el servicio encomendado fuera el de un servicio de atención al cliente en el que el encargado del tratamiento es el que mantiene el contacto directo con el interesado, sea este encargado el que deba cumplir con el deber de informar a estas personas[795].

Para que se realice este encargo del tratamiento deberá suscribirse un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento y que debe estipular que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable y que las obligaciones en materia de seguridad incumben a este encargado[796]. Por último, se especifica que la regulación que se incluya en el contrato o acto jurídico para cumplir con este precepto debe constar por escrito o en otra forma equivalente[797].

En la regulación del encargo del tratamiento de la Directiva 95/46/CE no se indica nada respecto a la posible subcontratación que pudiera llevar a cabo el propio encargado

[795] Otra cosa es que sea el responsable el que debe indicar concretamente cómo se cumplirá con este deber de informar. Otra obligación que claramente sería lógico que se pudiera delegar en el encargado es la atención del ejercicio de los derechos que se brindan al interesado, aunque una vez más debería especificarse cómo deberá cumplirse con este deber. En este sentido, la legislación española establece el supuesto en el que los interesados pudieran dirigirse al encargado del tratamiento para solicitar el ejercicio de algún derecho y establece que el encargado deberá dar traslado de esta solicitud al responsable, a no ser que en la relación con el responsable se prevea que el encargado atienda estas solicitudes por cuenta del responsable (art. 26 RLOPD).

[796] En Alemania el contenido que debe incluirse en el contrato entre el responsable y el encargado del tratamiento es mucho más amplio. Así se deben incluir los siguientes aspectos: el tipo y duración de los trabajos que deben realizarse, el alcance, tipo y fines de la recogida, tratamiento o uso de los datos, el tipo de datos y la categoría de interesados, las medidas de seguridad a adoptar, la rectificación, supresión y bloqueo de los datos, las obligaciones que se establecen en el mismo artículo que regula el contenido especialmente la monitorización, la capacidad de subcontratar, los derechos del responsable a monitorizar y las obligaciones correspondientes del encargado del tratamiento de aceptarlo y colaborar, las violaciones en la protección de los datos personales que realicen el encargado del tratamiento o sus empleados y que estén sujetas a la obligación de notificarlo, el alcance de la autoridad del responsable para dar instrucciones al encargado, la devolución de los soportes y la supresión de los datos registrados por el encargado después de que finalice el trabajo encargado (art. 11.2 Ley alemana). En la Ley checa se prima la ley como autorización para que el encargado lleve a cabo el tratamiento aunque también se establece la vía de que la autorización la otorgue el responsable mediante el contrato suscrito con este encargado que debe constar por escrito y que debe incluir el alcance, la finalidad y el período de tiempo por el que se suscribe y que debe establecer las garantías que debe reunir el encargado respecto a las medidas de seguridad de los datos (art. 6 Ley checa). Del mismo modo la Ley lituana sigue lo preceptuado al respecto del encargado de tratamiento por la Directiva 95/46/CE pero establece que no será necesario que se suscriba un contrato si la relación entre responsable y encargado está regulada por ley u otra disposición legal (art. 30.5 Ley lituana).

[797] La Ley islandesa incide en esta previsión al establecer que el contrato debe suscribirse por escrito y por duplicado y que responsable y encargado deben contar cada uno con su copia (art. 13 Ley islandesa).

del tratamiento del tratamiento objeto del encargo. Sin embargo, el hecho de que en la definición se incluya "solo o conjuntamente con otros" da a entender que podrá existir una pluralidad de encargados del tratamiento. No obstante, la definición parece apuntar a una posible contratación de varios encargados directamente por el responsable y no a través del encargado.

La falta de una regulación expresa relativa a esta posibilidad de subcontratación por parte del encargado del tratamiento en la Directiva 95/46/CE ha dado como resultado que, por lo general, no se haya abordado esta cuestión en las legislaciones nacionales. Como es evidente, en las leyes en las que se ha previsto algo al respecto los resultados han sido diversos al no contar con ninguna pauta[798].

Sin embargo, hay que decir que durante el proceso de elaboración de la Directiva 95/46/CE se estableció inicialmente que en el contrato se debía especificar una limitación para el encargado y sus empleados respecto a la comunicación de datos a terceros, de forma que sólo podrían realizarla si contaran con la autorización del responsable del tratamiento (art. 22.3 Propuesta de Directiva de 1990 y art. 24.3 Propuesta de Directiva de 1992). Esta previsión finalmente se eliminó del texto final.

El GA29 reconoce que es habitual que el responsable externalice el tratamiento de datos en varios encargados del tratamiento y que las nuevas tecnologías han propiciado estructuras enormemente complejas[799]. El grupo no ve nada en la Directiva 95/46/CE que impida que se pueda designar a varios encargados del tratamiento. No obstante, el GA29 especifica que todos estos encargados deberán ajustarse a sus instrucciones y deberá quedar clara la asignación de obligaciones y responsabilidades resultantes de la

[798] La Ley húngara prohíbe la subcontratación por parte del encargado del tratamiento (sección 10 Ley húngara). La Ley búlgara establece expresamente la posibilidad de que el responsable pueda contratar a más de un encargado del tratamiento, incluso cuando el único objetivo de esta contratación sea diferenciar las tareas (art. 24.1 Ley búlgara). No menciona la ley la posibilidad de que sea el encargado del tratamiento el que subcontrate otro encargado. La Ley croata establece como un aspecto que debe figurar en el contrato entre responsable y encargado del tratamiento la prohibición de comunicar datos a otros sujetos (art. 10 Ley croata). La Ley estonia establece que el encargado del tratamiento (*authorised processor*) podrá delegar el tratamiento de datos en otra persona si obtiene la autorización por escrito del responsable (*chief processor*) y si esto no excede los límites de la autoridad del encargado del tratamiento (*authorised processor*) (art. 7 Ley estonia). La Ley noruega establece que el encargado del tratamiento no podrá comunicar los datos a otra persona para su almacenamiento o manipulación sin el acuerdo del responsable (art. 15 Ley noruega). Por último mencionar la legislación española que ha establecido una regulación sobre la subcontratación (art. 21 RLOPD).

[799] Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.*, pág. 30.

legislación de protección de datos, de forma que no se difuminen a lo largo de la cadena de subcontratación[800].

Entiendo que el responsable deberá asegurar que mantiene el control sobre los fines y los medios esenciales del tratamiento en todo momento, también respecto a estos otros encargados subcontratados. El GA29 parece que amplía este necesario control a los elementos principales de la estructura del tratamiento que mencionan que pueden ser las partes implicadas, las medidas de seguridad o las garantías para el tratamiento en países terceros[801].

Además de ostentar unas obligaciones más limitadas que el responsable, en la Directiva 95/46/CE no se ha previsto la responsabilidad expresa del encargado del tratamiento, en caso de incumplimiento. El GA29 ha indicado que, aunque la Directiva 95/46/CE imponga únicamente la responsabilidad al responsable del tratamiento, no impide que las leyes nacionales dispongan también que el encargado del tratamiento deba responder en determinados supuestos[802]. No hay que olvidar que el encargado actúa en el marco de un mandato que además se formaliza obligatoriamente mediante un contrato por escrito o en otra forma equivalente (art. 17.4 Directiva 95/46/CE). Esto supone que si el encargado se extralimita de su mandato incumplirá el contrato y, por tanto, deberá responder por ello.

---

[800] *Ibídem.*
[801] *Ibídem.*
[802] *Ibídem.* La responsabilidad del encargado se ha establecido expresamente en la legislación española (art. 12.4 LOPD). En cambio, la Ley húngara especifica que el responsable responderá por la legitimación de sus instrucciones (sección 10 Ley húngara). La Ley búlgara señala que el responsable responderá de los daños causados a un tercero resultantes de los actos de comisión u omisión que cometiera el encargado del tratamiento (art. 24.5 Ley búlgara). La Ley estonia dispone que el responsable (*chief processor*) será responsable del cumplimiento por parte del encargado del tratamiento (*authorised processor*) de los requisitos de protección de datos (art. 7 Ley estonia). La Ley checa establece que, si el encargado del tratamiento detecta que el responsable incumple las obligaciones establecidas en la ley, debe notificárselo inmediatamente y cesar en el tratamiento de datos. Si no cumple con este precepto ambos, el responsable y el encargado, serán conjuntamente responsables por cualquier daño que pueda ocasionarse al interesado(art. 8 Ley checa). La Ley eslovena establece que si hubiera disputa entre responsable y encargado, este último está obligado a devolver los datos tratados en el marco del contrato ante el requerimiento del responsable. El encargado debe destruir inmediatamente o proporcionar las copias de los datos al órgano estatal competente por ley para la detección de infracciones penales, a tribunales u otros órganos estatales si así lo dispone la ley (art. 11.3 Ley eslovena). Cuando se cese al encargado, éste debe devolver los datos al responsable.

5.3. Las transferencias de datos a países terceros

Uno de los aspectos más importantes en la regulación contenida en la Directiva 95/46/CE es el de las transferencias internacionales de datos personales a otros países fuera del EEE, ya que permite completar la protección en aquellos casos que se escapan del ámbito de aplicación de la Directiva 95/46/CE. No obstante, el TJUE ha recordado su carácter de régimen especial, complementario, por lo tanto, del régimen general que establece el Capítulo II Directiva 95/46/CE relativo a la licitud de los tratamientos de datos[803]. A esto responde también la mención al necesario cumplimiento de las disposiciones de derecho nacional adoptadas con arreglo a las otras estipulaciones de la Directiva 95/46/CE[804].

El principio general en esta regulación es que no se podrán transferir datos a países que no cuenten con un nivel adecuado de protección (art. 25.1 Directiva 95/46/CE)[805]. Los Estados miembros y la Comisión deben informarse de los casos en que consideren que un país no garantiza un nivel de protección adecuada (art. 25.3 Directiva 95/46/CE). También se especifica que la Comisión podrá adoptar decisiones en las que establezca el nivel adecuado de protección de un país tercero[806], de acuerdo con los criterios que se establecen en la Directiva 95/46/CE (art. 25.6 Directiva 95/46/CE)[807].

---

[803] Sentencia del TJUE de 6 de noviembre de 2003, *Bodil Lindqvist*, C-101/01, EU:C:2003:596, apdo. 63. KUNER resalta la importancia de esta cuestión que muchos responsables olvidan. C. KUNER, *European data protection law, corporate compliance and regulation*, *op. cit.*, págs. 159 a 160.

[804] Así lo establece el artículo 25 Directiva 95/46/CE al indicar "sin perjuicio del cumplimiento de las disposiciones de derecho nacional adoptadas con arreglo a las demás disposiciones de la presente directiva" y el Considerando 60 que establece que "las transferencias hacia países terceros sólo podrán efectuarse si se respetan plenamente las disposiciones adoptadas por los Estados miembros en aplicación de la presente directiva y, en particular, de su artículo 8". El artículo 8 Directiva 95/46/CE es el que regula las categorías especiales de datos.

[805] En la Ley croata la regulación de las transferencias no se refiere únicamente a países terceros como destinatarios de los datos, sino también a organizaciones internacionales (art. 13 Ley croata).

[806] El listado de países sobre los que la Comisión ha adoptado decisiones en las que ha estimado su nivel adecuado se puede consultar en: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm, (fecha consulta: 3.11.2014). Como ejemplo de las decisiones adoptadas cabe citar especialmente por su importancia la relativa al nivel adecuado de EEUU: Decisión de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes publicadas por el Departamento de Comercio de Estados Unidos de América, DO nº L 215 de 25 de agosto de 2000.

[807] El artículo 25 Directiva 95/46/CE establece los criterios que se seguirán para evaluar el nivel de protección que ofrece el país destinatario de los datos. Debe atenderse a las circunstancias que concurran en la transferencia y en concreto: la naturaleza de los datos, la finalidad y duración del tratamiento, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero, así como las normas profesionales y las medidas de seguridad en vigor en dichos países. La Comisión y los Estados miembros se comunicarán los casos en que consideren que un país no garantiza un nivel adecuado.

Si la Comisión comprueba que un país no garantiza un nivel de protección adecuado, los Estados miembros deben adoptar las medidas necesarias para impedir las transferencias al mismo (art. 26.4 Directiva 95/46/CE)[808]. La Comisión podrá iniciar las negociaciones con el país controvertido para poder remediar esta situación (art. 26.5 Directiva 95/46/CE).

Como señala la propia Comisión Europea, las leyes nacionales han previsto de formas diferentes cómo se determina si existe un nivel adecuado de protección, de forma que, en algunos casos, incluso es el propio responsable el que realiza esta valoración[809]. También indica la Comisión que, respecto a sus decisiones sobre la adecuación del nivel de protección de países terceros, sólo una minoría de Estados miembros han reconocido

---

La Comisión podrá decidir sobre el nivel de protección de acuerdo con el procedimiento que establece la directiva en su artículo 31 que remite al establecido en la Decisión 1999/468/CE del Consejo, de 28 de junio de 1999, por la que se establecen los procedimientos para el ejercicio de las competencias de ejecución atribuidas a la Comisión, DO L 184 de 17.7.1999. En este procedimiento, la Comisión está asistida por un Comité compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión. Las medidas adoptadas por la Comisión en virtud de este procedimiento son de aplicación inmediata a no ser que el Comité no estuviera conforme, caso en el que se deberá comunicar la medida al Consejo que podrá adoptar una decisión diferente por mayoría cualificada. Los Estados miembros deberán adoptar las medidas necesarias para ajustarse a estas decisiones. Este procedimiento también se seguirá para la adopción por la Comisión de cláusulas contractuales que se consideren válidas para que las utilicen los responsables del tratamiento con el fin de ofrecer las garantías suficientes para que los Estados miembros autoricen la transferencia. En la regulación de las transferencias internacionales que estipula la Ley eslovena, resaltar que la autoridad de control podrá decidir que un país tiene el nivel adecuado de protección de forma total o parcial. La autoridad de control mantendrá un listado de estos países y para aquellos para los que haya decidido que sólo en parte aseguran este nivel de protección el listado establecerá en qué parte asegura este nivel (art. 66 Ley eslovena).

[808] De esta forma, como señala el GA29, se refuerza la seguridad jurídica y la uniformidad en toda la UE, ya que la Comisión adoptará decisiones sobre la adecuación del nivel de protección que serán válidas para todo el ámbito europeo. Cuando las decisiones sobre la adecuación las adopten las autoridades nacionales sólo tendrán eficacia en el ámbito nacional. Documento de trabajo del Grupo del Artículo 29 relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE, 2093/05/ES WP 114, 25.11.2005, Grupo de trabajo Artículo 29 sobre la protección de datos, págs. 5 a 6.

[809] *Commission Staff Working Paper, Impact assessment accompanying the document Regulation of the European Parliament […], op. cit.*, *Annex 2*, pág. 38. En la Ley inglesa se considera el octavo de los principios de protección de datos, establecidos en su anexo 1, la prohibición de transferir datos personales a un país o territorio fuera del EEE, a no ser que se asegure un adecuado nivel de protección para los derechos y libertades de los interesados, con relación al tratamiento de datos personales. Según indica KORFF, si no hay ninguna decisión sobre la adecuación del nivel de protección emitido por la Comisión Europea, la autoridad de control inglesa (el ICO) deja en manos del responsable que éste valore si el país tiene este nivel adecuado. D. KORFF, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Contract _r: JLS/2008/C4/011 – 30-CE-0219363/00-28, Country Studies, A.6-United Kingdom, op. cit*., pág. 68. La Ley croata establece que, en caso de que exista una duda razonable sobre la existencia de este nivel adecuado, el responsable deberá solicitar la decisión de la autoridad de control, de forma previa a realizar la transferencia (art. 13 Ley croata). Por tanto, también se permite que el responsable realice esta valoración.

su efecto directo, ya que en la mayoría de los casos se exigen medidas legislativas o administrativas para que estas decisiones tengan efecto[810].

Aunque un país no cuente con el nivel adecuado de protección, podrá ser de todas formas destino de la transferencia, si se puede aplicar alguna de las excepciones previstas (art. 26 Directiva 95/46/CE)[811]. También hay que tener en cuenta que se permite a los Estados miembros establecer "casos particulares" en los que no permitan la transferencia, aunque se puedan aplicar las excepciones. Las excepciones son las siguientes:

> "a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista[812], o b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o d) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta[813]."

[810] *Commission Staff Working Paper, Impact assessment accompanying the document Regulation of the European Parliament […], op. cit., Annex 2,* pág. 39.

[811] No obstante, en algunas leyes se establece un control adicional por parte de la autoridad de control, de forma que aunque el responsable considere que el supuesto encaja en alguna de estas excepciones, debe solicitar de todas formas el beneplácito de la autoridad de control (art. 20.1 Ley portuguesa, art. 9 Ley griega, art. 27.4 Ley checa, art. 29.3 Ley rumana que prevé la notificación previa a la autoridad de control).

[812] El GA29 ha interpretado que cualquier duda sobre el consentimiento no permitiría aplicar esta excepción. Así si a un individuo se le ha informado de la transferencia y no ha objetado, no puede considerarse que haya otorgado un consentimiento inequívoco. También aludía a que el consentimiento en el caso de transferencias estructurales y repetidas, como el hecho muy común por parte de multinacionales de centralizar la base de datos mundial de recursos humanos, implicaría situaciones de imposible solución si un empleado decidiera no consentir. Por ello, debería buscarse una solución alternativa, como la implantación de Reglas Corporativas Vinculantes (*Binding Corporate Rules*) o de contratos que permitan realizar la transferencia utilizando otro supuesto de legitimación. Documento de trabajo sobre transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la directiva de la UE sobre protección de datos, DG XV D/5025/98, WP12, de 24.7.1998, Grupo de trabajo Artículo 29 sobre la protección de datos, pág. 26; Documento de trabajo del Grupo del Artículo 29 relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE, *op. cit.*, pág. 13 y Dictamen 15/2011 del Grupo del Artículo 29, sobre la definición de consentimiento, *op. cit.*, págs. 30 a 31. Algunas leyes nacionales establecen que el consentimiento para realizar la transferencia sea expreso (así el artículo 30.a Ley rumana contempla que el consentimiento sea otorgado de forma explícita y por escrito y el artículo 36 Ley búlgara prevé que este consentimiento sea explícito).

[813] En algunas leyes se ha establecido una excepción que se refiere a aquellos datos que el interesado haya hecho manifiestamente públicos (art. 8.2.f Ley Liechtenstein, art. 29.6 Ley rumana).

El grado de armonización en las legislaciones nacionales deviene, una vez más, crucial para que los responsables que se ubiquen en los diferentes Estados miembros puedan llevar a cabo las transferencias en igualdad de términos[814]. De otra forma, se incentivan prácticas de *forum shopping*, al poder elegir el responsable el foro que le permita realizar las transferencias más fácilmente. En este sentido, el GA29 ha indicado que existen divergencias respecto a este listado de excepciones[815].

Si de todas formas el responsable no pudiera acogerse a ninguna de estas excepciones para poder realizar la transferencia internacional, aún existe otra posibilidad. Los Estados miembros pueden autorizar transferencias a países sin el nivel adecuado de protección si el responsable ofrece garantías suficientes respecto de la protección de los derechos de los interesados (art. 26.2 Directiva 95/46/CE). Un posible mecanismo que podrá utilizar el responsable para ofrecer estas garantías es la utilización de las cláusulas contractuales apropiadas que podrá suscribir con el sujeto importador de los datos en el extranjero[816]. La Comisión Europea podrá adoptar estas cláusulas contractuales tipo (art. 26.4 Directiva 95/46/CE)[817].

---

[814] La Ley estonia no permite todos los supuestos del listado de la Directiva 95/46/CE. En la Ley letona además de que se establecen las excepciones a la prohibición de transferir datos a países terceros que no cumplan con el nivel adecuado, de acuerdo con las excepciones que plantea la directiva, se añade al cumplimiento de la concreta excepción consistente en que el responsable debe supervisar que se cumplen las medidas de protección pertinentes (art. 28.2 Ley letona). Este requisito se traduce en que el responsable y el receptor de los datos deben suscribir un contrato relativo a la transferencia cuyos requisitos los determinará el Consejo de Ministros, si bien se especifica que quedarán fuera de este contrato las áreas de cooperación internacional, seguridad nacional y derecho penal (art. 28.4 Ley letona). También cabe resaltar que se establece que los datos personales pueden transferirse a otro estado de la UE o del EEE si ese país cumple con el nivel adecuado de protección, tal como se regula en la legislación en vigor de Letonia. Por tanto, en este país no se presume el nivel adecuado respecto a los Estados europeos (art. 28.5 Ley letona).

[815] El GA29, que remitía al primer informe de 2003 sobre la aplicación de la Directiva 95/46/CE, indicaba que existían diferencias en la aplicación de los artículos 25 y 26 Directiva 95/46/CE y del riesgo de que esto condujera al *forum shopping.* Documento de trabajo del Grupo del Artículo 29 relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE, 2093/05/ES WP 114, *op. cit.*, pág. 4.

[816] La Ley irlandesa establece que, en caso de que se realice la transferencia a un país tercero en virtud de que el responsable del tratamiento aporte como salvaguardia la utilización de cláusulas contractuales, de acuerdo con el artículo 26 apartados 2 y 4 de la Directiva 95/46/CE, el interesado podrá utilizar las cláusulas del contrato que le concedan derechos como si fuera parte del contrato. Se trata de dar plena eficacia a las cláusulas del contrato que se especifica que son en beneficio de terceros (los interesados) (art. 11.6 Ley irlandesa).

[817] Esta posibilidad de adopción de medidas de ejecución por parte de la Comisión seguirá el procedimiento al que remite el art. 31.2 Directiva 95/46/CE que se establece en la Decisión 1999/468/CE ya mencionada. Las decisiones adoptadas por la Comisión relativas a cláusulas contractuales tipo vigentes son: la Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE, DO L 181 de 4.7.2001 y la Decisión 2004/915/CE de la Comisión, que modifica la Decisión 2001/497/CE respecto a la introducción de unas cláusulas contractuales alternativas para la transferencia de datos personales a países terceros, DO L 385 de 29.12.2004, que se refieren ambas a las transferencias realizadas por parte de un responsable del tratamiento ubicado en el EEE hacia un responsable del tratamiento ubicado en un país tercero y la Decisión de la

Los Estados miembros deben informar a la Comisión y a los demás Estados miembros acerca de las autorizaciones que otorguen para la realización de transferencias de datos a países que no cuenten con el nivel adecuado. Además, se exige en este caso el seguimiento de un procedimiento que puede implicar incluso la oposición de algún Estado miembro a esta autorización (art. 26.3 Directiva 95/46/CE)[818].

El TJUE acude al contexto en el que se elaboró la Directiva 95/46/CE, para entender que el legislador europeo no pensaba en Internet cuando estableció este régimen relativo a las transferencias de datos. El tribunal europeo afirmó que no debía considerarse una transferencia de datos, tal como la contempla la Directiva 95/46/CE, la comunicación de los mismos por parte de una persona que los publique en Internet, de forma que sean accesibles desde todos los países del globo[819]. El TJUE evitó la aplicación de un régimen demasiado estricto que hubiera conllevado la imposibilidad de la utilización de Internet.

Comisión relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo C(2010)593 final, 5.2.2010; que se refiere a las transferencias que realice un responsable del tratamiento ubicado en el EEE hacia un encargado del tratamiento ubicado en un país tercero.

[818] En algunas leyes se establece esta obligación, como en el artículo 11.4 Ley irlandesa.

[819] La sentencia a la que se alude se produce en respuesta a una cuestión prejudicial al TJUE, que realizó el *Göta hovrätt* sueco sobre la interpretación de la Directiva 95/46/CE, en el marco de un proceso penal. La Sra. Lindqvist fue acusada de haber infringido la normativa sueca de protección de datos al publicar en su sitio de Internet datos de carácter personal sobre varias personas que, como ella, colaboraban voluntariamente con una parroquia de la Iglesia protestante de Suecia. Entre las cuestiones planteadas está la de si el tratamiento consistente en la difusión de datos personales por Internet, de modo que resulten accesibles a un grupo indeterminado de personas, debe considerarse como una transferencia de datos a países terceros. El TJUE entiende, mediante una forzada interpretación, que no estamos ante una transferencia internacional de datos. El tribunal argumenta que no puede presumirse que el legislador comunitario, en el momento de elaboración de la Directiva 95/46/CE, al regular las transferencias internacionales tuviera en cuenta el fenómeno de Internet. El estado del desarrollo de esta tecnología en ese momento y la ausencia de toda referencia a la misma en el capítulo IV dedicado a las transferencias dan soporte a esta interpretación. La ausencia de una definición de lo que debe considerarse una transferencia a un país tercero y la utilización de una infraestructura informática como paso necesario para poder publicar la información que evitan que se pueda hablar de transferencia directa entre dos personas también se utilizan como argumentos por el TJUE. Además si se interpretara que estamos ante una transferencia a un país tercero convertiría el régimen especial que contempla el capítulo IV, por lo que se refiere a Internet, en un régimen de aplicación general, ya que el funcionamiento de Internet implica que los datos se transmitan a países terceros. Esto implicaría que cuando uno solo de estos países terceros no garantizara el nivel de protección adecuado, los Estados miembros deberían impedir cualquier difusión de datos en Internet. Se trata, sin duda, de evitar un régimen demasiado estricto que conllevara la imposibilidad de la utilización de Internet. Sentencia del TJUE de 6 de noviembre de 2003, *Bodil Lindqvist*, C-101/01, EU:C:2003:596.

Sin embargo, esta sentencia no evita que deban aplicar esta regulación las empresas que utilizan recursos informáticos que, en muchas ocasiones se ubican en otros países. Es habitual que las multinacionales centralicen estos recursos y los servicios necesarios para mantenerlos. El hecho de tener que aplicar la regulación de las transferencias internacionales en estos grupos es una cuestión enormemente complicada[820].

En un intento por adaptar los mecanismos establecidos por la Directiva 95/46/CE para que permitan realizar transferencias de datos, en el actual panorama globalizado, se ha puesto en manos de los responsables del tratamiento una nueva herramienta: las reglas corporativas vinculantes (*Binding Corporate Rules* o BCR). Este instrumento ha surgido fruto de los trabajos del GA29[821].

[820] Esta complejidad la ilustra KUNER que ofrece una muestra de algunas de las arquitecturas contractuales que se utilizan habitualmente en el marco de las empresas multinancionales para poder suscribir las cláusulas tipo necesarias para poder tramitar las autorizaciones frente a las autoridades de control, para realizar las transferencias. C. KUNER, *European data protection law, corporate compliance and regulation*, *op. cit.*, págs. 204 a 208.

[821] El primer documento donde se plasmó este instrumento fue el documento de trabajo del GA29: *Document de travail: transferts de données personnelles vers des pays tiers: appliclation de l'article 26.2 de la directive de l'UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données, 11639/02/FR WP 74, 3.6.2003, Groupe de travail Article 29 sur la protection des données*. Después le siguieron la *Liste de contrôle type, demande d'approbation de règles d'entreprise contraignantes, 12110/04/FR WP 102, 25.11.2004, Groupe de travail Article 29 sur la protection des données*; *Document de travail relatif à une procédure de coopération en vue de l'émission d'avis communs sur le caractère adéquat de la protection offerte par les "règles d'entreprise contraignantes", 05/FR WP 107, 14.4.2005, Groupe de travail Article 29 sur la protection des données* y el *Document de travail établissant une liste de contrôle type pour les demandes d'approbation des règles d'entreprise contraignantes, 05/FR WP 108, 14.4.2005, Groupe de travail Article 29 sur la protection des données*, considerándose el WP 74 y el WP 108 los documentos básicos sobre el instrumento. Después se han complementado con otros documentos para facilitar su utilización por los responsables del tratamiento: *Recommendation 1/2007 on the standard application for approval of binding corporate rules for the transfert of personal data, WP 133, 10.1.2007, Article 29 Working Party; Document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes, 1271-00/08/FR WP 153, 24.6.2008, Groupe de travail Article 29 sur la protection des données; Document de travail établissant un cadre pour la structure des règles d'entreprise contraignantes, 1271-00-01/08/FR WP 154, 24.6.2008, Groupe de travail Article 29 sur la protection des données; Document de travail sur les questions fréquemment posées (FAQ) concernant les règles d'entreprise contraignantes, 1271-04-02/08/FR, WP 155 rév. 04, 24.6.2008, revisé 8.4.2009, Groupe de travail Article 29 sur la protection des données.* La Ley de Liechtenstein recoge también este mecanismo, ya que se refiere a la posibilidad de comunicar datos en el seno de la misma persona jurídica o compañía o entre personas jurídicas o compañías que están bajo el mismo liderazgo, siempre que sus participantes estén sujetos a unas reglas comunes de protección de datos que aseguren una adecuada protección (art. 8.2.g Ley de Liechtenstein). Sin embargo, tanto este supuesto, como el que permite que el responsable utilice cláusulas contractuales para asegurar la protección de los derechos de los interesados exigen además la autorización del gobierno, aunque la autoridad de control emitirá de forma previa una recomendación sobre si se garantiza la protección adecuada con las reglas (art. 8.2.a Ley de Liechtenstein).

Las reglas corporativas vinculantes hallan su fundamento en las políticas corporativas que elaboran las empresas multinacionales para armonizar la forma de gestionar ciertos aspectos a nivel de todas las compañías integrantes del grupo. Lo que se perseguía con las BCR era facilitar las transferencias de datos entre las empresas integrantes del grupo multinacional, de forma que no tuvieran que solicitar autorizaciones en los diferentes países en los que se ubicaran.

Mediante la adopción de las reglas corporativas vinculantes, el grupo multinacional garantiza que las transferencias se realizan como si se suscribieran entre todas las empresas las cláusulas contractuales que permiten asegurar el nivel adecuado de protección. El procedimiento de solicitud de autorización para realizar transferencias de datos a países terceros se simplifica, porque la solicitud, para realizar las mismas mediante las BCR, se presenta a la autoridad de control donde se halle la sociedad matriz del grupo y en virtud de la colaboración entre las diferentes autoridades de control que estén implicadas se tramita la autorización o autorizaciones necesarias[822]. No obstante, hay que tener en cuenta que no todas las autoridades forman parte del sistema de reconocimiento mutuo[823].

También este mecanismo ha evolucionado, de forma que ahora se trabaja en el seno del GA29 para la utilización de las BPR, es decir, las *Binding Processor Rules* o reglas corporativas para encargados del tratamiento[824]. De esta forma, se posibilita que los encargados del tratamiento puedan elaborar estas reglas corporativas vinculantes con el objetivo de que en el seno del su grupo multinacional se puedan realizar transferencias internacionales de datos.

[822] Por tanto, el trabajo del GA29 se ha centrado en desarrollar esta colaboración entre las autoridades de control para hacer posible este mecanismo.

[823] Los países que participan en este sistema de reconocimiento mutuo son: Austria, Bélgica, Bulgaria, Chipre, República Checa, Estonia, Francia, Alemania, Islandia, Irlanda, Italia, Letonia, Liechtenstein, Luxemburgo, Malta, Países Bajos, Noruega, Eslovaquia, Eslovenia, España y el Reino Unido. http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/mutual_recognition/index_en.htm (Fecha consulta: 14.8.2015).

[824] Los documentos que ha dedicado por el momento el GA29 a esta cuestión son: el *Document de travail 02/2012 établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes pour les sous-traitants, 930/12/FR WP 195, 6.6.2012, Groupe de travail Article 29 sur la protection des données*; la *Recommendation 1/2012 on the standard application form for approval of binding corporate rules for the transfer of personal data for processing activities, WP 195a, 17.9.2012, Article 29 Data Protection Working Party; Explanatory document on the Processor Binding Corporate Rules, 00658/13/EN WP 204 rev.01, 19.4.2013, revised and adopted on 22.5.2015, Article 29 Data Protection Working Party*.

De todas formas, el responsable del tratamiento seguirá obligado a solicitar la autorización para realizar las transferencias internacionales de datos. Sin embargo, podrá presentar como documentación para realizar este trámite el contrato suscrito con el encargado del tratamiento y las BPR que este encargado haya sometido al procedimiento de aprobación del GA29.

Otro paso más que el GA29 ha dado en esta materia es la elaboración de un borrador de cláusulas contractuales *ad hoc*, que sugiere el grupo, podría aprobar la Comisión para favorecer los trámites de autorización de transferencias internacionales de datos[825]. Este clausulado serviría para transferencias internacionales de datos entre un encargado del tratamiento europeo y un sub-encargado del tratamiento ubicado en un país fuera del EEE que no cuente con el nivel adecuado de protección. Este clausulado debería partir de un previo acuerdo marco, que deberían suscribir el encargado del tratamiento y el responsable del tratamiento, de forma que se asegurara el control por parte de este último en todo momento[826].

Por último, el GA29 también ha instaurado la posibilidad de poner en marcha un procedimiento de cooperación entre las autoridades de control europeas, similar al de las BCR pero para revisar contratos elaborados en virtud de las cláusulas tipo aprobadas por la Comisión[827]. El objetivo de este procedimiento es evitar incoherencias en los análisis que puedan efectuar las diferentes autoridades de control del mismo contrato, en los casos en que grupos de empresas utilicen una misma versión del contrato para solicitar autorización en diferentes Estados. Este procedimiento podrá iniciarlo la empresa que someterá el modelo que quiere autorizar a la autoridad líder y será revisado por todas las que estén implicadas en las transferencias. De nuevo, la sujeción a este procedimiento es voluntario por parte de las autoridades. Ya ha utilizado este procedimiento *Amazon*[828], que solicitó al GA29 que le revisara un modelo de contrato que quería utilizar con sus

[825] *Working document 1/2014 on draft ad hoc contractual clauses "EU data processor to non-EU sub-processor", 757/14/EN WP 214, 21.3.2014, Article 29 Data Protection Working Party*.
[826] Este clausulado se originó de la iniciativa de la AEPD que, como se comentará en el siguiente capítulo, presentó en el año 2012 este tipo de clausulado y, de hecho, ya ha concedido autorizaciones en virtud del mismo.
[827] *Working document setting forth a co-operation procedure for issuing common opinions on "contractual clauses" considered as compliant with the EC model clauses, 14/EN WP 226, 26.11.2014, Article 29 Data Protection Working Party*.
[828] *Amazon Web Services, Whitepaper on EU data protection, april 2015*, pág. 5, https://d0.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper_EN.pdf (fecha consulta: 21.8.2015)

clientes. La autoridad de control de Luxemburgo le respondió que estimaban que el clausulado cumplía con la Decisión de la Comisión 2010/87/UE[829].

6. DERECHOS O FACULTADES

Hay que decir que la Directiva 95/46/CE no recoge expresamente derechos del responsable del tratamiento. Sin embargo, se pueden deducir lo que podríamos considerar derechos o facultades que el responsable del tratamiento adquiere ligados a las obligaciones expuestas. El hecho de que se establezca una obligación que debe cumplir el responsable, implica que si, a su vez, se incluyen excepciones a la misma, se podrán considerar estas excepciones habilitaciones de las que gozará el responsable.

Sin embargo, algunas de estas habilitaciones excepcionales también se apoyan en derechos o intereses legítimos del responsable, lo que les brinda una mayor relevancia. Por ello, tras enumerar los derechos o facultades que se pueden identificar en la regulación de la Directiva 95/46/CE, me referiré al derecho a tratar datos que entiendo supone uno de estos supuestos. Asimismo, mencionaré el derecho a someter proyectos de códigos de conducta a las autoridades de control, por la importancia de este mecanismo pese a su escasa utilización.

6.1. La asignación de derechos o facultades

De la regulación de la Directiva 95/46/CE se pueden extraer los siguientes derechos o facultades del responsable que, en el ciclo lógico del tratamiento se refieren a la fase de entrada: derecho a tratar datos personales si se acoge a alguno de los supuestos de legitimación establecidos en la directiva (art. 7 Directiva 95/46/CE) y a tratar categorías especiales de datos si se acoge a alguno de los supuestos de legitimación establecidos en la directiva para este tipo de datos (art. 8 Directiva 95/46/CE); acogerse a las posibles exenciones y excepciones que establezcan los Estados miembros para permitir el tratamiento de datos con fines exclusivamente periodísticos o de expresión

[829] La autoridad de control de Luxemburgo, que fue designada como autoridad líder en este caso, publicó una carta de 6.3.2015, en la que consideraba que el modelo presentado por Amazon se adaptaba a la Decisión de la Comisión 2010/87/UE. http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/AWS-3-6-15.pdf (fecha consulta: 21.8.2015)

artística o literaria (art. 9 Directiva 95/46/CE); respecto a la obligación de notificar a la autoridad de control los tratamientos (art. 18 Directiva 95/46/CE) podrá acogerse a la simplificación o a la omisión del requisito si así lo disponen los Estados miembros en la regulación.

Respecto a los derechos o facultades que se podrían calificar de transversales están los siguientes: respecto a la obligación de no someter a una persona a una decisión con efectos jurídicos que se adopte únicamente en virtud de un tratamiento automatizado de datos, los responsables podrán someter a esa persona a la decisión indicada si concurren los requisitos establecidos (art. 15 Directiva 95/46/CE); podrán someter los proyectos de códigos de conducta o las modificaciones o prórrogas de los mismos a examen de las autoridades nacionales (art. 27.2 Directiva 95/46/CE) o al GA29 si el código es de alcance europeo; respecto a la obligación de someterse a los poderes de investigación e intervención de las autoridades de control (art. 28.3 Directiva 95/46/CE) tienen derecho a que los miembros y agentes de las autoridades de control estén sujetos al deber de secreto profesional sobre las informaciones confidenciales a las que hayan tenido acceso (art. 28.7 Directiva 95/46/CE).

En la fase de salida incluiríamos que, respecto a la obligación de no realizar transferencias a países que no garantizan el nivel adecuado de protección (art. 25 Directiva 95/46/CE), los responsables podrán llevarlas a cabo si se acogen a alguno de los supuestos enunciados en la directiva (art. 26 Directiva 95/46/CE).

6.2. El derecho del responsable a tratar datos

La habilitación para tratar datos personales que permite el encaje en alguno de los supuestos establecidos por la Directiva 95/46/CE hace que nos planteemos si puede considerarse que el responsable tiene un derecho a tratar datos personales. Más que un derecho directo a tratar datos, lo que cabe argumentar es que el responsable tiene un derecho indirecto o una facultad para realizar este tratamiento. Esta facultad dimana de la legitimación para tratar datos que derivará, como se ha analizado, de alguna de las bases jurídicas enunciadas en el artículo 7 Directiva 95/46/CE. Es más acertado hablar de facultad en lugar de derecho, porque en algunos supuestos será más bien una obligación de tratar datos.

Hay que recordar que la Directiva 95/46/CE nace para asegurar la construcción del mercado interior de la UE y, por tanto, la protección de datos se origina como un problema a esta construcción desde una perspectiva mercantilista[830]. Lo que pretende esta norma es asegurar que los responsables podrán tratar datos personales y hacerlos circular sin problemas en el marco de este mercado interior.

Si una ley establece una obligación que debe cumplir el responsable y, para ello, es necesario que lleve a cabo un tratamiento de datos, tendrá la obligación más que el derecho de tratar datos. Una ley que obliga a tratar datos personales es la misma Directiva 95/46/CE. Así, el TJUE a la hora de determinar el alcance del derecho de acceso que tienen los interesados, ha considerado que debe referirse a datos tratados en un momento previo al ejercicio del derecho[831]. Por tanto, surge la obligación del responsable de conservar esos datos durante un intervalo de tiempo, cuya determinación se ha dejado en manos de los Estados miembros. Esta determinación del intervalo deberá asegurar un equilibrio entre el interés del afectado en acceder a estos datos y la carga que esta obligación puede representar para el responsable del tratamiento[832].

Otro ejemplo puede ser el del Tribunal de cuentas austríaco (*Rechnungshof*), que reclamaba que los organismos bajo su control le entregaran los datos relativos a las retribuciones y pensiones superiores a un nivel determinado, que estos organismos abonaban a sus empleados y pensionistas[833]. El objetivo, establecido en una ley federal, era elaborar un informe que se transmitía a los diversos Parlamentos a nivel federal y estatal y que se ponía también a disposición del público. Algunos de estos organismos se negaron a proporcionar esta información porque entendían que era contrario a la Directiva 95/45/CE y al derecho a la vida privada que contempla el artículo 8 CEDH.

El Tribunal de cuentas austríaco reclamaba su derecho a tratar datos en virtud de una previsión legal que así lo contemplaba. En definitiva, esta percepción del tratamiento

[830] A. RALLO LOMBARTE, "Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma", *UNED, Revista de derecho político*, nº 85, septiembre-diciembre 2012, pág. 22.
[831] Sentencia del TJUE de 7 de mayo de 2009, *College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer*, C-553/07, EU:C:2009:293.
[832] *Ibídem*, (apdos 64 y 66).
[833] Sentencia del TJUE de 20 de mayo de 2003, *Rechnungshof/Österreichischer Rundfunk* y otros C-465/00, C-138/01 y C-139/01, EU:C:2003:294.

de datos como un derecho deriva de la naturaleza de la base jurídica escogida, que es la que realmente se configurará como un derecho u obligación. El tratamiento de datos será una actividad ligada a esta base jurídica y accesoria a la misma.

Si el responsable se apoya en la base jurídica relativa a la satisfacción de su interés legítimo (art. 7.f) Directiva 95/46/CE) el tratamiento de datos puede hallar su fundamento en un derecho de los establecidos en la Carta UE, como pueden ser el derecho a la libertad de empresa o el derecho a la libertad de información[834]. De hecho, en referencia al interés legítimo, la Directiva 95/46/CE menciona el desempeño de actividades legítimas de gestión ordinaria de empresas y otras entidades (Considerando 30 Directiva 95/46/CE), lo que enlazaría con el derecho a la libertad de empresa[835]. El responsable podrá alegar que precisa tratar datos personales para poder cumplir con este derecho, aunque lo cierto es que, como ha sucedido en el asunto *Google*, este interés se suele poner por detrás del derecho de los interesados a la protección de datos[836].

Otra cuestión importante que debe tener en cuenta el responsable va más allá de la legalidad y tiene que ver con la protección multinivel de los derechos fundamentales. Y es que, aunque el responsable se aferre a una base jurídica para poder tratar datos personales, puede ver cómo se la ponen en duda, en virtud del artículo 8.2 CEDH o del artículo 52.1 Carta UE, al considerarse una limitación al derecho de protección de datos.

---

[834] De esta forma el Abogado General en el asunto *Google* aludía a estos derechos para primar el interés legítimo del buscador de *Google* a tratar datos personales. Conclusiones del Abogado General Niilo Jääskinen de 25 de junio de 2013 en el asunto *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:201:424, apdo. 95. Asimismo, en el asunto *Satamedia*, el TJUE indica que los derechos que protege la Directiva 95/46/CE deben conciliarse con el derecho fundamental a la libertad de expresión, necesidad que se refleja en el artículo 9 y en el Considerando 37 Directiva 95/46/CE, conciliación que incumbe a los Estados miembros. Para ello los Estados miembros deben prever excepciones o restricciones a la protección de datos y, por lo tanto, al derecho a la intimidad previstos en los capítulos II, IV y VI de la Directiva. Sentencia del TJUE de 16 de diciembre de 2008, *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy, Satamedia Oy*, C-73/07, EU:C:2008:727, apdos. 53 a 55.

[835] La libertad de empresa que se enuncia en el artículo 16 Carta UE se considera que, en abstracto, abarca la libertad de iniciativa económica y la libertad de acceso al mercado, la libertad de decisión que se refiere a la autonomía organizativa y de gestión empresarial, la libertad de competencia y la libertad de cese de la actividad. Este contenido se delimita y concreta por el legislador que podrá restringirlo en virtud de otros principios y derechos. P. MERCADO PACHECO, "Artículo 16. Libertad de empresa", C. MONEREO ATIENZA, J.L. MONEREO PÉREZ (Dir. Coord.), VVAA, *La Europa de los derechos. Estudio sistemático de la Carta de los derechos fundamentales de la Unión Europea*, Comares, Granada, 2012, pág. 380.

[836] El TJUE califica de mero interés económico el interés legítimo del gestor del motor de búsquedas y enseguida lo descarta ante la gravedad de la injerencia producida. Tiene más en cuenta en la valoración el interés de los internautas en el acceso a la información del buscador. Sentencia del TJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2014:317, apdo. 81.

Para ilustrar este planteamiento, se puede acudir de nuevo a la cuestión prejudicial planteada en el asunto *Rechnungshof*. El TJUE entendió que existía injerencia en el derecho a la vida privada de los trabajadores y pensionistas afectados y tuvo que valorar, si esta injerencia, prevista en la normativa, era justificada, de acuerdo con lo establecido en el artículo 8.2 CEDH[837]. La respuesta del TJUE fue que la normativa que establecía el tratamiento de datos sólo podía justificarse si era necesaria y apropiada para lograr el objetivo de mantener los salarios dentro de unos límites razonables, aunque remitía a los órganos jurisdiccionales nacionales para que lo valoraran[838].

Según el TJUE, si los tribunales nacionales consideraran la normativa incompatible con el CEDH, entonces ya no podría cumplir con la exigencia de proporcionalidad establecida en la Directiva 95/46/CE, cuando exige que los datos sean recogidos con fines determinados, explícitos y legítimos (art. 6.1.b) Directiva 95/46/CE), así como adecuados, pertinentes y no excesivos con relación a los fines (art. 6.1.c) Directiva 95/46/CE) y cuando indica que su tratamiento será lícito si es necesario para el cumplimiento de una obligación jurídica o para una misión de interés público o inherente al ejercicio del poder público (art. 7.c) y e) Directiva 95/46/CE)[839].

En definitiva, de nuevo se advierte el papel del responsable de garante del derecho, de forma que tiene que ir más allá de la propia legalidad, para evitar futuros conflictos. Su seguridad jurídica dependerá de la calidad de las leyes que enmarcan su actividad, ya sea, del sector público o privado. En este sentido, sería importante reclamar también un principio de *privacy by law*, de privacidad desde la legislación, al igual que la *privacy by design*. El legislador no sólo debe contar con las autoridades de control, que emiten informes cuando se detecta que hay una repercusión en el derecho, sino que tendría que tener en cuenta esta perspectiva multinivel de protección del derecho.

[837] El TJUE, por tanto, analizó si se cumplían los requisitos del artículo 8.2 CEDH: previsión legal y medida que, en una sociedad democrática, sea necesaria para los fines establecidos (la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral o la protección de los derechos y libertades de los demás). Sentencia del TJUE de 20 de mayo de 2003, *Rechnungshof/Österreichischer Rundfunk* y otros C-465/00, C-138/01 y C-139/01, EU:C:2003:294, apdos. 73-75.
[838] Sentencia del TJUE de 20 de mayo de 2003, *Rechnungshof/Österreichischer Rundfunk* y otros C-465/00, C-138/01 y C-139/01, EU:C:2003:294, apdo. 90.
[839] *Ibídem*, apdo. 91.

El responsable también debe tener en cuenta que esta facultad habilitante de tratar datos se haya constreñida al resto de la regulación de la Directiva 95/46/CE y, especialmente a los principios de calidad que se enuncian en su artículo 6 Directiva 95/46/CE. Asimismo, en función de estos principios en los que se exige que el tratamiento de datos sea lícito se deberá respetar también el marco legal vigente que le sea aplicable. Como ya se ha indicado previamente, el derecho a la protección de datos es transversal y debe tener en cuenta el marco legislativo en el que se incardina el tratamiento de datos.

6.3. El derecho a someter un código de conducta a las autoridades de control

Entre las facultades que la Directiva 95/46/CE atribuye al responsable del tratamiento está la de poder someter los proyectos de códigos de conducta o las modificaciones o prórrogas de los mismos a examen de las autoridades nacionales (art. 27.2 Directiva 95/46/CE) o al GA29 si el código es de alcance europeo.

Se trata de una manifestación de la utilización por parte del Estado de mecanismos de autorregulación regulada, de forma que se quiere alentar a los responsables a que se autorregulen, para adaptar mejor sus actividades a la normativa. Un repaso de las obligaciones que deben cumplir los responsables deja entrever la complejidad del cumplimiento de esta legislación. Por ello, lo que se pretendía con los códigos es que los responsables que se movieran en un mismo sector elaboraran un conjunto de reglas que les facilitara el cumplimiento al adaptar la regulación general a su sector concreto[840]. Esta forma de autorregulación debía ser verificada por las autoridades de control.

Sin embargo, esta primera piedra en el proceso de incentivación de la autorregulación no ha tenido el éxito que se buscaba, especialmente en lo que se refiere a códigos de ámbito europeo[841]. Este poco éxito a nivel europeo es fácilmente explicable ya que adoptar un código que tenga ese ámbito de aplicación y que debe respetar, por tanto,

[840] El Considerando 61 Directiva 95/46/CE es el que refleja este objetivo, de forma que dispone que tanto los Estados miembros como la Comisión deben alentar a los sectores profesionales para que elaboren estos códigos y faciliten la aplicación de la directiva, habida cuenta del carácter específico el tratamiento.

[841] Ello pese a que rápidamente el GA29 dió las pautas para el examen de estos códigos. Labor futura en relación con los códigos de conducta: documento de trabajo sobre el procedimiento de examen de los códigos de conducta comunitarios por el Grupo de Trabajo, DG XV D/5004/98 WP 13, 10.9.1998, Grupo de trabajo Artículo 29 sobre la protección de datos.

las legislaciones que transponen la Directiva 95/46/CE en los diferentes Estados miembros, es complicado[842]. Además el GA29 en su evaluación del código revisa que, además de cumplirse con la legislación, se proporcione un valor añadido, de forma que se adopten enfoques específicos a los tratamientos de datos contemplados[843]. Como resultado sólo se ha aprobado un código europeo de la Federación Europea de Marketing Directo (FEDMA)[844].

En lo que respecta a la transposición de esta posibilidad en las leyes nacionales de protección de datos, de nuevo hay que señalar las diferencias en las aproximaciones. De esta forma, al lado de leyes que ni siquiera han contemplado esta posibilidad[845] otras han revestido a los códigos de conducta de un especial reforzamiento[846].

---

[842] La única manera es acudir a fórmulas que se incluyen en el código en las que se deja claro que pueden haber algunos aspectos que contradigan lo que establece la legislación nacional por lo que es necesario, al final que los responsables conozcan bien la normativa que les aplica, por lo que se pierde el beneficio que persiguen los códigos de facilitar el cumplimiento de estas normas. Ejemplo de estas fórmulas es el que se introdujo en el Código de conducta europeo de la FEDMA "*All provisions of this code apply without prejudice to the provisions of the applicable national legislation. Where specific requirements exist at national level, this will have to be complied with in accordance with the applicable law rules set out in this Code and in accordance with EU legislation*." Anexo al Dictamen 3/2003 relativo al Código de conducta europeo de la FEDMA sobre la utilización de datos personales en la comercialización directa, 10066/03/ES final WP 77, 13.6.2003, Grupo de trabajo Artículo 29 sobre la protección de datos.

[843] Dictamen 3/2003 relativo al Código de conducta europeo de la FEDMA sobre la utilización de datos personales en la comercialización directa, *op. cit.*, p.3. Destaca la rigurosidad de este proceso de aprobación al que achaca el poco éxito en la elaboración de códigos: J. VIGURÍ CORDERO, J., "Los mecanismos de certificación (códigos de conducta, sellos y marcas)", A. RALLO LOMBARTE, R. GARCÍA MAHAMUT (Ed.), VVAA, *Hacia un nuevo derecho europeo de protección de datos. Towards a new European data protection regime*, *op. cit*., pág. 921.

[844] Este código se presentó al GA29 en 1998 y no fue aprobado hasta el 2003 mediante el Dictamen 3/2003 relativo al Código de conducta europeo de la FEDMA sobre la utilización de datos personales en la comercialización directa, *op. cit.*. No obstante, en ese dictamen el GA29 solicitó a FEDMA que incorporara un anexo para resolver algunas cuestiones que quedaron pendientes, y este anexo no fue aprobado hasta el año 2010 mediante el Dictamen 4/2010 relativo al «Código de conducta europeo de la FEDMA sobre la utilización de datos personales en la comercialización directa», 00065/2010/ES WP 174, 13.7.2010, Grupo de trabajo Artículo 29 sobre la protección de datos.

[845] No contemplan la aprobación de códigos de conducta la Ley húngara, la Ley eslovena, la Ley letona, la Ley lituana ni la Ley checa.

[846] El artículo 12 Ley italiana establece la necesidad de que la autoridad de control italiana (el *Garante)* impulse le elaboración de códigos de conducta sectoriales. Además se especifica que se realizará siguiendo las recomendaciones del Consejo de Europa y que el cumplimiento con lo establecido en los códigos será un requisito para que el tratamiento que lleven a cabo las entidades del sector privado o público sea considerado lícito, por lo que se refuerza su aplicación. Hay que entender que este apartado se refiere a aquellas entidades adheridas al código. La Ley búlgara establece que la autoridad de control debe coordinar por sector industrial y por área de actividad, los códigos de conducta de responsables de datos personales (art. 10.4 y 22a Ley búlgara). La autoridad de control debe incentivar, según la Ley maltesa, la elaboración de un código de conducta específico que debe aplicarse a los periodistas y medios de comunicación para regular el tratamiento de datos personales que llevan a cabo (art. 6 Ley maltesa). En caso de que no se elabore este código, la autoridad de control podrá establecer medidas específicas para proteger a los interesados. Además, en caso de que no se cumplan los preceptos del código, la autoridad de control podrá prohibir el tratamiento de datos y ordenar el bloqueo de los datos cuando exista un riesgo grave de daño a los interesados.

CAPÍTULO VI

EL ESTATUTO DEL RESPONSABLE EN LA LEGISLACIÓN ESPAÑOLA

Una vez visto el estatuto del responsable en la Directiva 95/46/CE y en las legislaciones nacionales europeas, corresponde examinar el abanico de obligaciones y derechos o facultades que esta figura tiene en la legislación española[847]. En este caso, se seguirá también el ciclo lógico del tratamiento de datos.

1. LA ASIGNACIÓN DE OBLIGACIONES

En la legislación española, si bien las obligaciones que se estipulan con el fin de proteger el derecho a la protección de datos no se asignan siempre expresamente, queda claro que el responsable o el encargado del tratamiento son los principales destinatarios de las mismas, ya que el régimen de infracciones que recoge la LOPD sólo contempla como posibles responsables a estas dos figuras. El recorrido por las obligaciones se realizará respecto a aquellas asignadas al responsable[848].

Respecto a la dualidad entre responsable del tratamiento y responsable del fichero, no parece que las menciones que se realizan en los textos legales y, especialmente en la LOPD, se refieran concretamente a cada una de estas figuras de forma estricta, ya que como se ha abordado, esta diferenciación surgió de la jurisprudencia y se plasmó en el RLOPD[849].

En consecuencia, aunque el RLOPD parece haber seguido la distribución de papeles realizada por la LOPD, no puede decirse que este reparto sea lo suficientemente sólido para que pueda aplicarse en la práctica. También hay que tener en cuenta que esta diferenciación entre ambas figuras está en desuso, excepto para algunos ámbitos concretos. Por tanto, llevar a cabo una clasificación en función de esta dualidad estimo

[847] El trabajo se centrará en el estudio de las obligaciones que aparecen en la LOPD y el RLOPD, aunque hay que tener en cuenta que en algunas normativas sectoriales se incorporan disposiciones relativas a la protección de datos.
[848] Si bien el examen no se centra en las obligaciones que implican infracción, aunque, evidentemente, en su mayoría existirá coincidencia.
[849] Ver Capítulo III.

que no sería útil e incluso confusa[850]. Por tanto, examinaré las obligaciones, sin atender al tipo exacto de responsable al que se asignan, excepto si ello fuera relevante por establecer una responsabilidad específica de ese sujeto.

Otra mención necesaria es la de aquellos roles que crea la normativa que se superponen a los de responsable o encargado. Estos papeles se asignan en ámbitos concretos de la regulación. Así, cuando se hace referencia a las transferencias internacionales se establecen los conceptos de exportador e importador (art. 5.1.j) y ñ) RLOPD). En la regulación de las fuentes accesibles al público, se crea el papel de entidad responsable del mantenimiento de estas fuentes (art. 28 LOPD). También cuando se alude al destinatario o cesionario (art. 5.1.h) RLOPD) habitualmente se hará referencia a un responsable.

A las entidades promotoras de los códigos tipo (art. 78 RLOPD), en virtud de las funciones asignadas por la normativa, no se les asignaría el papel de responsables. Pese a eso, se les asignan unas determinadas obligaciones, aunque su incumplimiento entiendo que tampoco conllevará sanción.

Hay otros sujetos obligados que se mencionan en la regulación, pese a que no pueden ser sancionados y que forman parte de la organización del responsable. Estos sujetos son las personas que intervengan en cualquier fase del tratamiento que están obligados a guardar secreto profesional respecto a los datos a los que accedan (art. 10 LOPD). Asimismo, en la parte que dedica el RLOPD al desarrollo de las medidas de seguridad que deben adoptar el responsable y el encargado (Título VIII RLOPD), también son sujetos que intervienen en esta regulación: el responsable de seguridad y los usuarios.

Respecto a la asignación de las obligaciones del responsable que se extraen de la LOPD[851] y que se refieren a la fase de entrada de datos serían: recoger el consentimiento

[850] Para dar una idea de la dificultad, baste señalar que el RLOPD distribuye las obligaciones entre las siguientes variantes de responsable: el responsable del tratamiento, el responsable del fichero, el responsable, el responsable del fichero y tratamiento, el responsable del fichero común y el titular del fichero común o titular.

[851] Las obligaciones se encuentran en la LOPD, principalmente, en el Título II, dedicado a los "Principios de la protección de datos", en el Título III, que se refiere a los "Derechos de las personas", en el Título IV, donde se incluyen las disposiciones sectoriales relativas a ficheros de titularidad pública y a ficheros de titularidad privada y en el Título V referente al "Movimiento internacional de datos".

preciso para poder llevar a cabo el tratamiento de datos personales o hacerlo de acuerdo con otro de los supuestos que legitiman el tratamiento (arts. 6, 22.2, 28, 29.1 y .2, 30.1 LOPD); tratar los datos especialmente protegidos de acuerdo con las limitaciones establecidas (arts. 7, 8, 22.3 LOPD); cumplir con el deber de información (arts. 5, 24, 29.2, 30.2 LOPD) y cumplir con los requisitos establecidos para la creación, modificación o supresión de ficheros (arts. 20, 25, 26 LOPD).

Las obligaciones transversales que se refieren a todo el ciclo lógico del tratamiento son: respetar el principio de calidad de los datos (arts. 4, 22.4, 29.4 LOPD); respecto a los derechos que tienen los interesados, el responsable debe: atender el derecho de oposición (arts. 6.4, 30.4 LOPD) y la revocación del consentimiento (art. 6.3 LOPD); no someter a los ciudadanos a decisiones con efectos jurídicos adoptadas en virtud de tratamientos de datos destinados a evaluar aspectos de su personalidad, atender la impugnación de las decisiones o actos administrativos que impliquen una valoración del comportamiento y proporcionar información si el afectado lo solicita sobre los criterios de valoración y el programa utilizados en este tipo de tratamientos (art. 13 LOPD); atender el ejercicio de los derechos de acceso, rectificación y cancelación (arts. 15, 16, 17, 23, 29.3, 30.3 LOPD); indemnizar al afectado si el responsable incumple la ley (art. 19 LOPD). El responsable también tendrá que adoptar las medidas que garanticen la seguridad de los datos (art. 9 LOPD); respetar el deber de secreto (art. 10 LOPD); atender los requerimientos o apercibimientos de la AEPD o proporcionar cuantos documentos e informaciones sean solicitados por la misma y no obstruir el ejercicio de la función inspectora (arts. 37.1.f) e i) y 40.1 LOPD).

Las obligaciones relativas a la fase de salida de datos son: cumplir con el régimen específico aplicable a la comunicación de datos (art. 11, 21, 27 LOPD) y con los requisitos establecidos para poder permitir el acceso a datos a encargados del tratamiento (art. 12 LOPD); no realizar transferencias de datos a países que no proporcionen un nivel de protección equiparable al establecido por la LOPD, excepto si se obtiene la autorización previa del Director de la AEPD o se puede aplicar alguna excepción (art. 33 y 34 LOPD).

2. OBLIGACIONES EN LA FASE DE ENTRADA DE LOS DATOS PERSONALES

Antes de iniciar el tratamiento es esencial que el responsable realice un proceso previo de análisis de todos los aspectos implicados en el tratamiento de datos personales. Esta será la forma de conseguir una estrategia de adaptación a lo establecido en la normativa que sea coherente en todas sus facetas, desde el inicio del ciclo del tratamiento hasta el final.

2.1. La legitimación para tratar datos

A diferencia de la Directiva 95/46/CE, que incorpora todos los supuestos que legitiman los tratamientos de datos en un solo precepto (art. 7 Directiva 95/46/CE), en la LOPD debe acudirse a diversos artículos (principalmente arts. 6 y 11 LOPD). El principal motivo de esta diversificación es la separación que la normativa española ha realizado de una modalidad de tratamiento concreta: la cesión o comunicación de datos[852]. En la Directiva 95/46/CE no se diferencia entre las operaciones que conforman el concepto de tratamiento de datos y, por ello, la regulación es uniforme para todas ellas[853]. Esta dispersión de las bases jurídicas del tratamiento se ha intentado reparar mediante su refundición en el artículo 10 RLOPD.

Otra divergencia de la LOPD respecto a la Directiva 95/46/CE, es que, mientras ésta enumeraba los supuestos de legitimación sin que ninguno sobresaliera sobre el otro[854], la LOPD dispone como supuesto destacado el consentimiento (de hecho, el art. 6 LOPD se titula "consentimiento del afectado") sobre los demás supuestos. La relevancia del mismo ha sido puesta de manifiesto por el Tribunal Constitucional que ha considerado

[852] La Comisión Europea destacaba esta complejidad en la regulación española al diferenciar la cesión de datos respecto a las demás modalidades de tratamiento, añadido a la defectuosa transposición del artículo 7.f Directiva 95/46/CE que abordaré más adelante, en su primer informe sobre la adaptación de los Estados miembros a la directiva: *"This peculiarity together with the fact that the Spanish law confers a special treatment to processing that consists of disclosure of information to a third party* ("cesion de datos") *makes the processing of personal data without consent of individuals considerably more difficult in Spain than in other countries" Analysis and impact study on the implementation of Directive EC 95/46 in Member States, Annex to "First report on the implementation of the Data Protection Directive (95/46/EC)", COM(2003) 265 final, Brussels, 15.5.2003*, pág.11.

[853] Si bien en algunos artículos sí que se hace referencia explícita a la cesión. Ver Capítulo V.

[854] Ver Capítulo V.

el consentimiento como una de facultades que el derecho de protección de datos atribuye a sus titulares y que forman parte del núcleo esencial del mismo[855].

Como excepciones a la regla general del consentimiento para tratar datos, se establecen los siguientes supuestos: que la ley habilite el tratamiento de datos; que los datos se recojan para el ejercicio de las funciones propias de las Administraciones públicas, en el ámbito de sus competencias; que los datos se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; que el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7.6 LOPD.

A estas excepciones deberá añadirse el supuesto establecido en el artículo 7.f) Directiva 95/46/CE al considerarse de aplicación directa por el TJUE para corregir la incorrecta transposición realizada por la LOPD de este precepto[856]. Por tanto, también podrán tratarse datos si es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado.

Asimismo, en las disposiciones sectoriales relativas a ficheros de titularidad pública y privada se encuentran concreciones de los supuestos de legitimación que también habrá que tener en cuenta (arts. 22.2, 29.1 y .2, 30.1 LOPD). Respecto a los ficheros de titularidad privada también se establece la posibilidad que tienen las personas, empresas o entidades "titulares" de crearlos, cuando esto resulte necesario para el logro de su actividad u objeto legítimos y se respeten las garantías que establece la LOPD (art. 25 LOPD). Por tanto, la creación de los ficheros será preciso que se enmarque en estos objetivos y la referencia al titular debe entenderse realizada al responsable del fichero.

[855] En concreto, el TC ha considerado que el derecho atribuye "la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular". STC 292/2000, de 30 de noviembre de 2000, FJ 7.

[856] Sentencia del TJUE de 24 de noviembre de 2011, *ASNEF, FECEMD/Administración del Estado*, C-468/10 y C-469/10, EU:C:2011:777.

A continuación, se incidirá en los supuestos, en concreto que habilitan el tratamiento, excepto en lo relativo al supuesto referido al interés vital del interesado, que se abordará en el apartado dedicado a los datos especialmente protegidos.

2.1.1. El consentimiento

La LOPD establece que "el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa" (art. 6.1 LOPD). La definición de consentimiento de la LOPD es equivalente al de la Directiva 95/46/CE, con la única diferencia de añadir el adjetivo "inequívoca": "consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen." (art. 3.h) LOPD). No obstante, a efectos prácticos esta diferencia no tendrá importancia puesto que la Directiva añade este calificativo posteriormente en sede de legitimación[857].

En lo que respecta a las características del consentimiento relativas a libre, específico e informado se pueden aplicar los criterios interpretativos que alegaba el GA29[858]. Hay que destacar la importancia de la información que el Tribunal Supremo ha calificado de elemento consustancial a la prestación del consentimiento[859]. El cumplimiento de este requisito deberá entenderse alcanzado si se respeta lo exigido por el deber de informar (art. 5 LOPD)[860].

El GA29 cuestionaba si la ausencia de una acción o una acción pasiva podían interpretarse compatibles con la exigencia de encontrarnos ante una "manifestación de

[857] En el artículo 7.a) Directiva 95/46/CE que se refiere a los supuestos que podrán legitimar el tratamiento de datos personales: "Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: a) el interesado ha dado su consentimiento de forma inequívoca, (…)"

[858] Ver Capítulo V.

[859] El Tribunal Supremo, en una sentencia que admite recurso de casación por unificación de doctrina relativa a un consentimiento informado sanitario, se refiere a la LOPD. El Alto Tribunal indica que la LOPD pone de manifiesto el carácter consustancial que el elemento de la información tiene con la prestación de consentimiento respecto a la disposición de datos personales, tanto en su definición de consentimiento como en el artículo 11.3 LOPD cuando dispone que "será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar". STS de 18 de junio de 2004 (Sala 3ª) (ROJ: STS 4258/2004), FJ 1.

[860] J.M. FERNÁNDEZ LÓPEZ, "Principio de consentimiento", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, *op. cit.*, pág. 458.

voluntad" y con el requisito de que el consentimiento sea inequívoco. Por tanto, el GA29 ponía en duda que se pudiera acudir a un consentimiento tácito. La normativa española, por el contrario, contempla claramente como admisible el consentimiento tácito, lo que cabe colegir del establecimiento de la regla de consentimiento expreso para el tratamiento de los datos especialmente protegidos (art. 7 LOPD)[861]. Debe entenderse que si el legislador hubiera querido que el consentimiento exigido para cualquier tratamiento de datos debiera revestir esta característica de expreso, lo habría especificado, tal como ha hecho para el caso de este tipo de datos en concreto[862]. Lo mismo se puede decir de la forma escrita que también se exige para recoger el consentimiento en algunos de los datos especialmente protegidos, por lo que debe entenderse que no debe exigirse en el resto de casos.

Pero es que además se recoge en el RLOPD una fórmula de consentimiento tácito, salvo cuando la ley exija que éste sea expreso (art. 14 RLOPD). Esta fórmula consiste en dirigirse al afectado para cumplir con el deber de información y concederle un plazo de treinta días para que pueda manifestar su negativa al tratamiento. Este supuesto corresponde a un ejemplo que el GA29 consideraba que no cumpliría con los requisitos exigidos al consentimiento[863].

Respecto a la palabra "específico", que alude a la granularidad del consentimiento que debe otorgarse respecto a cada uno de los diferentes aspectos del tratamiento de datos, se establece que "la solicitud de consentimiento deberá ir referida a un tratamiento

[861] También lo ha entendido así la Audiencia Nacional. SAN de 5 de mayo de 2008 (Sala de lo contencioso-administrativo) (ROJ: SAN 523/2008), FJ 3.

[862] Como indica FERNÁNDEZ LÓPEZ, que el legislador sea riguroso a la hora de valorar la existencia de consentimiento no debe confundirse con la forma en que el consentimiento se manifiesta. J.M. FERNÁNDEZ LÓPEZ, "Principio de consentimiento", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, *op. cit.*, pág. 455. Así lo indica también la Audiencia Nacional, que considera que "el artículo 6.1 de la LOPD no exige que el consentimiento revista una forma determinada pero sí que no admita duda o equivocación, pues éste y no otro es el significado del adjetivo utilizado para calificar tal consentimiento de inequívoco". SAN de 6 de mayo de 2011(Sala de lo contencioso-administrativo) (ROJ: SAN 2198/2011), FJ 4.

[863] El GA29 pone un ejemplo en el que un responsable envía una carta a sus clientes en la que indica que transferirá sus datos a no ser que se opongan en el plazo de dos semanas. Si sólo le responde un 10% de los clientes, puede ser bastante dudoso que el 90% de los que no respondieron acepten la transferencia. El GA29 pone de manifiesto que la ambigüedad de esta respuesta pasiva hará difícil cumplir con los requisitos de la Directiva y además el responsable no tendrá evidencias de este consentimiento. Dictamen 15/2011, sobre la definición de consentimiento, *op. cit.*, pág. 14. La Audiencia Nacional ha admitido que el envío de una publicación reiteradamente sin haber manifestado el destinatario su oposición ni habe devuelto las publicaciones recibidas, suponía la existencia de consentimiento tácito a ese tratamiento. SAN de 5 de mayo de 2008 (Sala de lo contencioso-administrativo) (ROJ: SAN 523/2008), FJ 3.

o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos" (art. 15 RLOPD). No obstante, se admite que cuando se quiera solicitar el consentimiento, durante el proceso de formación de un contrato, para poder tratar datos para finalidades que no guarden relación directa con el mismo, se pueda hacer dando la oportunidad al afectado de que en ese momento se niegue al tratamiento, por ejemplo, mediante la marcación de una casilla (art. 15 RLOPD).

El RLOPD incluye una referencia en su artículo 13 al consentimiento para el tratamiento de menores de edad, especialmente interesante para el contexto digital. El consentimiento para poder tratar estos datos deberá exigirse a los mayores de catorce años[864]. En el caso de menores de esta edad se requerirá el consentimiento a los padres o tutores. Serán los titulares de la patria potestad o la tutela quienes presten este consentimiento cuando la ley establezca la necesidad de esta asistencia para mayores de catorce años, en alusión al tratamiento de los datos de los incapacitados.

Este precepto prohíbe la recogida de datos a través del menor que puedan referirse a su familia, con la excepción de aquellos datos que sean precisos para recabar la autorización si fuera necesario, tal como se indicaba anteriormente. Asimismo, se exige que la información que se ofrezca a los menores se exprese en un lenguaje fácilmente comprensible para ellos y que se adopten procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado por sus representantes. La utilización de estos procedimientos es lo que conlleva mayor dificultad en los entornos *online*[865].

[864] No obstante PÉREZ LUÑO advierte de la necesidad de tener en cuenta respecto al ejercicio del consentimiento del menor la garantía del interés superior del menor que puede implicar la adopción de medidas paternalistas en contra de la autonomía del mismo. Este conflicto debe resolverse al atender al grado de madurez del menor que podría no coincidir con la edad establecida para prestar consentimiento. A.E. PÉREZ LUÑO, "El consentimiento de los menores", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.,* págs. 487 a 488.

[865] Así lo señalan en el contexto de las redes sociales ARENAS RAMIRO y MARTÍNEZ MARTÍNEZ y destacan que uno de los escollos es la imposibilidad de utilizar el DNI electrónico. Posteriormente a estas reflexiones se ha aprobado el Real Decreto 869/2013, de 8 de noviembre, por el que se modifica el Real Decreto 1553/2005, de 23 de diciembre, que regula la expedición del documento nacional de identidad y sus certificados de firma electrónica (BOE núm. 281 de 23.11.2013). Uno de los objetivos de esta modificación es dar respuesta a esta dificultad y, por ello, entre las modificaciones que incluye se establece en esta norma que para los menores de edad o que no tengan capacidad de obrar, el documento nacional de identidad incluya la utilidad de la identificación electrónica. Por tanto, si bien no se solventa el problema, ya que exigirá la utilización de este DNI, al menos el primer paso se ha dado. M. ARENAS RAMIRO, "La validez del consentimiento en las redes sociales on line", A. RALLO LOMBARTE, R. MARTÍNEZ

2.1.2. La habilitación legal

La LOPD establece como primera excepción al requisito del consentimiento del afectado para poder tratar datos, que la ley disponga otra cosa (art. 6.1 LOPD). Esta previsión que podía entenderse referida únicamente a la propia LOPD como ley habilitante, se precisa en el RLOPD que especifica que será posible el tratamiento o la cesión de los datos cuando lo autorice una norma con rango de ley o una norma de derecho comunitario (10.2.a RLOPD). El RLOPD establece dos supuestos que, en particular, podrán incluirse en este caso de autorización legal cuando:

> "El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.
> El tratamiento o la cesión sean necesarios para que el responsable del tratamiento cumpla con un deber que le imponga una de dichas normas" (art. 10.2.a RLOPD).

Estos dos supuestos responden, tanto al contenido positivo, como al negativo que pueden contemplar las normas respecto al responsable. Es decir, tanto si la norma lo que ampara es la satisfacción de un interés legítimo, como si lo que establece es un deber para el responsable, permitirán que éste pueda llevar a cabo el tratamiento de datos. La Directiva 95/46/CE contemplaba únicamente el contenido negativo, ya que indicaba que el tratamiento debía ser necesario para cumplir una obligación jurídica a la estuviera sujeto el responsable (art. 7.c) Directiva 95/46/CE) ¿Por qué se contempla entonces el interés legítimo amparado en una ley?

En este caso se conectan dos supuestos de legitimación del tratamiento: la ley y el supuesto de interés legítimo (art. 7.f) Directiva 95/46/CE). Como se comentará más adelante, el RLOPD había incluido en su artículo 10.1.b) una transposición incorrecta de

---

MARTÍNEZ (Ed.) VVAA, *Derecho y redes sociales*, 2ª ed., Aranzadi, Cizur Menor (Navarra), 2013, págs. 183 a 184 y R. MARTÍNEZ MARTÍNEZ, "Menores y redes sociales. Condiciones para el cumplimiento del artículo 13 del Reglamento de desarrollo de la Ley Orgánica de protección de datos", A. RALLO LOMBARTE, R. MARTÍNEZ MARTÍNEZ (Ed.) VVAA, *Derecho y redes sociales*, *op. cit.*, pág. 224. Respecto al procedimiento de verificación implementado en la red social española Tuenti dirigida a menores, ver N. MARTOS DÍAZ, O. CASADO OLIVA, "Políticas de privacidad, redes socials y protección de datos. El problema de la verificación de edad. Sistemas de autorregulación", A. RALLO LOMBARTE, R. MARTÍNEZ MARTÍNEZ (Ed.) VVAA, *Derecho y redes sociales*, *op. cit.*, págs. 251 a 255.

este artículo 7.f) Directiva 95/46/CE, tal como dictaminó el TJUE[866]. Sin embargo, el Tribunal Supremo decidió no interpelar al TJUE sobre el artículo 10.2.a) RLOPD, pese a que también repetía el supuesto de interés legítimo sobre que el que versaba la petición judicial.

El Tribunal Supremo explicó la no inclusión de este artículo en las cuestiones prejudiciales porque estimó que no existía confrontación entre el RLOPD y la Directiva 95/46/CE, ya que el precepto sólo añadía al texto de ésta última que el supuesto debía estar autorizado por una norma. El Alto Tribunal consideró que lo que contemplaba el RLOPD era otro supuesto habilitador que, pese a no encontrarse expresamente previsto en la Directiva 95/46/CE, no restringía la regulación de la misma. Sin embargo, apuntaba que podría limitarse el supuesto de la Directiva, si la ley nacional habilitadora estableciera condiciones a lo que establece el artículo 7.f) Directiva 95/46/CE[867]. Si la lista que ofrece el artículo 7 Directiva 95/46/CE es una lista exhaustiva[868], debería haber sido anulado este supuesto, en aras de una mayor claridad de la regulación, de por sí compleja y además cuando el artículo 7.c) Directiva 95/46/CE también goza de efecto directo[869].

Respecto al supuesto en que la ley imponga un deber al responsable que haga necesario el tratamiento o la cesión de datos, el RLOPD aclara que no es preciso que lo que la norma imponga sea el tratamiento en sí, sino que basta con que lo que imponga sea un deber que precise de ese tratamiento de datos. Se trata de una precisión lógica ya que no siempre el legislador establecerá expresamente el tratamiento de datos que debe llevar a cabo el responsable[870].

La habilitación para tratar datos, como señala la Carta UE se puede encontrar en un fundamento legítimo previsto por la ley[871]. Estas leyes deberán cumplir con los

[866] Sentencia del TJUE de 24 de noviembre de 2011, *ASNEF, FECEMD/Administración del Estado*, C-468/10 y C-469/10, EU:C:2011:777.
[867] STS de 8 de febrero de 2012 (Sala 3ª) (ROJ: STS 429/2012) FJ 6.
[868] Sentencia del TJUE de 24 de noviembre de 2011, *ASNEF, FECEMD/Administración del Estado*, C-468/10 y C-469/10, EU:C:2011:777, apdo. 30.
[869] Sentencia del TJUE de 20 de mayo de 2003, *Rechnungshof/Österreichischer Rundfunk* y otros C-465/00, C-138/01 y C-139/01, EU:C:2003:294.
[870] Así lo comenta respecto a la cesión de datos A. TRONCOSO REIGADA, "La comunicación de datos personales", en A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, *op. cit.*, pág. 967.
[871] El artículo 8.2 Carta UE establece que: "2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto

requisitos establecidos para los límites a los derechos fundamentales[872]. En esta disposición se entenderán incluidos todos los supuestos que habilita la misma LOPD en sus disposiciones sectoriales relativas a los ficheros o tratamientos de las Fuerzas y cuerpos de seguridad, de solvencia patrimonial y crédito y de publicidad[873].

2.1.3. Las funciones propias de las administraciones públicas

La LOPD establece que los datos deben ser recogidos para el ejercicio de las funciones propias de las administraciones públicas en el ámbito de sus competencias (art. 6.2 LOPD) y el RLOPD añade que estas competencias deben ser atribuidas por una norma con rango de ley o una norma de derecho comunitario (art. 10.3.a) RLOPD) ¿Por qué se añadió esta habilitación legal que remite a otra fuente de legitimación? La respuesta parece que hay que hallarla en la STC 292/2000, de 30 de noviembre de 2000. Esta sentencia, que reconoció el derecho de protección de datos, como derecho autónomo, también declaró inconstitucional, entre otros preceptos, un inciso del artículo 21.1 LOPD. Esta disposición prohibía que las administraciones públicas pudieran comunicar datos personales a otras administraciones para el ejercicio de competencias diferentes o que versaran sobre materias distintas, salvo cuando hubieran previsto estas comunicaciones en sus disposiciones de creación del fichero, o en disposiciones de superior rango, que regularan su uso.

El TC declaró este inciso inconstitucional porque entendió que la LOPD, en vez de regular ella misma los límites al derecho, renunciaba a ello y apoderaba a las administraciones públicas para que pudieran establecerlos ellas mediante disposiciones infralegales[874]. En consecuencia, el TC consideró que se había vulnerado la reserva de ley (arts. 53.1 y 81.1 CE)[875].

---

por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación." (El subrayado es de la autora).

[872] STC 292/2000, de 30 de noviembre de 2000, FJ 14.

[873] Si bien, veremos cuando se analice el supuesto del interés legítimo que también se han considerado estas regulaciones consecuencia de establecer legalmente habilitaciones en virtud de esa base jurídica. En definitiva entiendo que, de acuerdo con la normativa española, serían supuestos que pueden encajarse en ambas bases jurídicas: ley o interés legítimo.

[874] STC 292/2000, de 30 de noviembre de 2000, FJ 11.

[875] *Ibídem*.

Sin embargo, se ha criticado esta declaración de inconstitucionalidad que obliga a que las comunicaciones de datos para ejercer competencias distintas deban establecerse en leyes, ya que no sucedía lo mismo con la recogida de datos, que no contenía, como se ha visto, ninguna referencia a que las competencias de las administraciones, que permiten tratar datos, tuvieran que estar previstas por ley[876]. De hecho, la amplitud que permitía el artículo 6.2 LOPD también se había criticado, por entender que anulaba la regla del consentimiento[877]. Con el añadido del RLOPD se ha querido precisar, en coherencia con el pronunciamiento del TC, que las competencias también debían respetar esta garantía legal[878].

2.1.4. La relación contractual

Con el desarrollo efectuado por el RLOPD de esta excepción se aclaró la dicción de la LOPD[879]. No será preciso el consentimiento cuando los datos se recaben "con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que debe ser parte el interesado y sean necesarios para su mantenimiento o cumplimiento" (art. 10.3.b RLOPD). El hecho de que este supuesto se configure como una excepción a la regla general del consentimiento ha sido criticado por entenderse que, en cualquier caso, supone el otorgamiento del consentimiento, necesario para la perfección del contrato[880].

[876] Si bien es cierto que las administraciones se hayan sometidas al principio de legalidad (art. 103 CE). Muy crítico con la declaración de inconstitucionalidad ha sido A. TRONCOSO REIGADA, *La protección de datos personales. En busca del equilibrio*, *op. cit.*, págs. 144 a 168.

[877] Así lo consideraba M.M. SERRANO PÉREZ, *El derecho fundamental a la protección de datos. Derecho español y comparado*, Civitas, Madrid, 2003, págs. 210 a 214.

[878] L.M. ARROYO YANES, "Las administraciones públicas y la excepción al principio de prestación del consentimiento por parte del interesado a la recogida y tratamiento de sus datos personales", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, *op. cit.*, págs. 542 a 543.

[879] La LOPD indica "contrato o precontrato de una relación negocial, laboral o administrativa" (art. 6.2 LOPD), por lo que resulta algo confuso.

[880] En este sentido, cabe citar a APARICIO SALOM, que alude a la aplicación del art. 1.258 Cc, según el que el consentimiento prestado para la perfección de un contrato obliga "no sólo al cumplimiento de lo expresamente pactado, sino también a todas las consecuencias que, según su naturaleza, sean conformes a la buena fe, al uso y a la ley" y del art. 1.256 Cc, según el que "la validez y el cumplimiento de los contratos no pueden dejarse al arbitrio de uno de los contratantes". Por tanto, este autor indica que debe considerarse el tratamiento de datos un elemento esencial para la ejecución y el cumplmiento del contrato, por lo que debe entenderse que el consentimiento para tratar datos se ha otorgado con la aceptación de la oferta del contrato. J. APARICIO SALOM, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, 4ª ed, *op. cit.*, pág. 179.

La dificultad de aplicar este supuesto radica en evaluar qué datos serán necesarios para el mantenimiento o cumplimiento de la relación jurídica, lo que además se conectará con el principio de calidad (art. 4 LOPD). El responsable deberá analizar el marco jurídico de esa relación para determinar los datos que podrá tratar.

2.1.5. La satisfacción del interés legítimo del responsable

En este apartado es obligado mencionar la sentencia del TJUE, que estableció la incorrecta transposición del artículo 7.f) Directiva 95/46/CE por la legislación española y, más concretamente por el artículo 10.2.b RLOPD, que era del que partía el Tribunal Supremo para interponer la cuestión prejudicial[881].

El artículo 7.f) Directiva 95/46/CE permite tratar datos si se reúnen dos requisitos acumulativos: la satisfacción del interés del responsable o el tercero y que no prevalezca el interés del interesado. Al requerir una ponderación entre estos intereses a este supuesto se le conoce como el test del equilibrio o ponderación de intereses (*balance of interest*). El artículo 10.2.b) RLOPD recogía estos requisitos, pero además establecía que los datos debían figurar en fuentes accesibles al público.

El Tribunal Supremo planteó si este requisito adicional relativo a las fuentes accesibles al público era compatible con lo establecido por la Directiva 95/46/CE. Hay que tener en cuenta que las fuentes accesibles al público vienen tasadas en la LOPD y son únicamente: el censo promocional, los repertorios telefónicos, los listados de profesionales, los Diarios y Boletines oficiales y los medios de comunicación (art. 3.j) LOPD). El TJUE respondió que este requisito no se incluía en la Directiva 95/46/CE y lo que hacía era excluir de forma categórica y generalizada todo tratamiento que no figurara en tales fuentes[882]. Además el TJUE también aclaró que el artículo 7.f) Directiva 95/46/CE tenía efecto directo. Ello implica que esta disposición puede ser invocada por un particular y aplicada por los órganos jurisdiccionales.

[881] Sentencia del TJUE de 24 de noviembre de 2011, *ASNEF, FECEMD/Administración del Estado*, C-468/10 y C-469/10, EU:C:2011:777, en respuesta a las peticiones de decisión prejudicial planteadas por el Tribunal Supremo español en el marco del procedimiento contencioso-administrativo iniciado por la Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y la Federación Española de Comercio Electrónico y Marketing Directo (FECEMD) contra diversos artículos del RLOPD.

[882] Sentencia del TJUE de 24 de noviembre de 2011, *ASNEF, FECEMD/Administración del Estado*, C-468/10 y C-469/10, EU:C:2011:777, apdo. 49 y fallo.

Hay que indicar que esta sentencia del TJUE no fue ninguna sorpresa, ya que el defecto en la transposición del artículo 7.f) Directiva 95/46/CE por el ordenamiento español ya se había detectado en el primer informe sobre la transposición de la Directiva de la Comisión Europea, que consideraba que no se había incluido el precepto en la legislación española[883]. En este sentido, algunos autores defendían que este supuesto de interés legítimo también se hallaba incorporado en otros preceptos de la LOPD[884].

El Tribunal Supremo acogió la interpretación del TJUE y anuló el artículo controvertido del RLOPD, el 10.2.b), al entender que la circunstancia de que los datos figuren en fuentes accesibles al público no actuaba como elemento de ponderación, sino como un requisito habilitante que se adicionaba a los establecidos por el artículo 7.f) Directiva 95/46/CE[885]. Asimismo, pese a que el Tribunal Supremo no se pronunció sobre

[883] En el marco de este informe, el gobierno español, indicó que, en virtud del criterio de interés legítimo, se habían establecido aquellos supuestos en los que prevalecía el interés de los responsables para llevar a cabo el tratamiento. Estos supuestos eran los relativos a información sobre crédito, seguros y el tratamiento de datos de fuentes accesibles al público: "*The situation in Spain in this regard is also peculiar. The absence of this provision in the Spanish Data Protection Law is justified by the government, in the sense that the legislator, similarly to the Finnish one, sets out those cases where the balance test authorises controllers to carry out the processing of personal data. Consequently, in Spain, such processing operations would be those necessary for credit reporting purposes, insurance purposes (e.g. aimed at identifying fraud) and any operations involving the processing of certain type of data which would be made publicly available from the so-called publicly available sources such as the promotional census, the telephone directories, official journals, etc." Analysis and impact study on the implementation of Directive EC 95/46 in Member States, Annex to "First report on the implementation of the Data Protection Directive (95/46/EC)", COM(2003) 265 final, Brussels,* 15.5.2003, pág. 11. La Comisión volvía a incidir en este defecto en la transposición de este criterio del artículo 7.f) Directiva 95/46/CE en el ordenamiento español, en los anexos al Estudio de Impacto realizado a raíz de la reforma de la Directiva. De esta forma se especifica que España y Grecia imponen requisitos más estrictos para los tratamientos que se llevan a cabo en virtud de este criterio. Sin embargo, este estudio no recoge el fallo de la sentencia comentada del TJUE que salvaría este defecto. *Commission Staff Working Paper, Impact assessment accompanying the document Regulation of the European Parliament […], op. cit., Annex 2,* pág. 27.

[884] Así lo señalaba PUENTE ESCOBAR, en respuesta a la apreciación de la Comisión Europea realizada en el primer informe de 2003 mencionado sobre la no incorporación de la previsión del artículo 7.f) de la Directiva 95/46/CE en la legislación española. Este autor estimaba que la LOPD ya reconocía la concurrencia de un interés legítimo como presupuesto habilitante del tratamiento de datos en tres supuestos: la referencia al concepto de "relación jurídica" en los artículos 6.2 y 11.2.c) LOPD, la remisión a la habilitación legal prevista en los artículos 6.1 y 11.2.a) LOPD y la referencia expresa al "interés legítimo" y el equilibrio de intereses en el tratamiento de datos contenidos en fuentes accesibles al público según los artículos 6.2 y 11.2.b) LOPD. A. PUENTE ESCOBAR, "Legitimación para el tratamiento", R. MARTÍNEZ MARTÍNEZ (Coord.). *Protección de datos: comentarios a la LOPD y su reglamento de desarrollo, op. cit.*, pág. 22.

[885] STS de 8 de febrero de 2012 (Sala 3ª) (ROJ: STS 429/2012), FJ 7. Como ejemplo se puede mencionar un supuesto en el que la Audiencia Nacional revoca una resolución de la AEPD en la que había sancionado a un colegiado, cabeza de lista en unas elecciones colegiales, a quien el Colegio profesional le había entregado un listado de colegiados, en el que se incluía la dirección de correo electrónico, para que enviara información sobre su candidatura. Respecto a este dato la AEPD consideró que debía solicitarse el consentimiento porque no se entendía incluido en la fuente accesible al público. La Audiencia considera

esta cuestión, por entender que no era competente[886], al declararse el efecto directo del artículo 7.f) Directiva 95/46/CE también hay que entender que no se aplicará el artículo que originó el artículo 10.2.b) RLOPD que es el artículo 6.2 *in fine* LOPD[887].

2.2. Datos especialmente protegidos

A diferencia de lo que sucedía en la Directiva 95/46/CE, en la LOPD, los supuestos que habilitan el tratamiento de los datos considerados especialmente protegidos, se contienen en una regulación independiente y específica para estos tratamientos (arts. 7 y 8 LOPD). Por tanto, para tratar este tipo de datos no sería precisa la aplicación acumulativa de los supuestos de legitimación generales (art. 6 LOPD). La configuración de esta regulación es totalmente diferente de lo que establece la Directiva 95/46/CE y también, como veremos los requisitos establecidos para tratar datos.

Los datos que se consideran especialmente protegidos son aquellos que revelen la ideología, afiliación sindical, religión, creencias y los que hagan referencia al origen racial o étnico, a la salud, a la vida sexual y los datos relativos a la comisión de infracciones penales o administrativas (art. 7 LOPD)[888]. Sólo se ha incluido la definición de lo que se considera datos de carácter personal relacionados con la salud, entre los que se encuentran los datos genéticos, al mismo tiempo que se han dejado fuera los datos biométricos[889].

---

que el colegiado ostentaba un interés legítimo en el tratamiento de datos y que éste debía prevalecer. SAN de 31 de mayo de 2012 (Sala de lo contencioso-administrativo) (ROJ: SAN 2747/2012), FJ 4.

[886] *Ibídem*, FJ 2.

[887] Así lo ha entendido la SAN de 11 de abril de 2012 (Sala de lo contencioso-administrativo) (ROJ: SAN 1702/2012), FJ 6. El artículo 6.2 in fine LOPD establece: "o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado." De esta forma, se entenderá que se inaplica el requisito relativo a las fuentes accesibles al público que subrayo.

[888] El listado de la LOPD contiene algunas diferencias respecto al de la Directiva 95/46/CE. De esta forma, en vez de opiniones políticas, en la LOPD se hace referencia a ideología; en vez de convicciones religiosas o filosóficas, se indica en la LOPD religión o creencias; en vez de pertenencia a sindicatos, la LOPD se refiere a afiliación sindical; en lugar de datos relativos a la salud o a la sexualidad, se habla de datos que hacen referencia a la salud y a la vida sexual; en vez de datos relativos a infracciones, condenas penales o medidas de seguridad se hace referencia a datos relativos a comisión de infracciones penales o administrativas. Estos matices en los que difieren los términos pueden dar cabida a una interpretación más amplia o más estricta que permita diferencias entre la interpretación que se pueda hacer de los mismos de acuerdo con la Directiva 95/46/CE o de acuerdo con la LOPD.

[889] Así, se consideran datos de carácter personal relacionados con la salud las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información

Se establece la prohibición de crear ficheros con la finalidad exclusiva de almacenar datos de carácter personal de las categorías enumeradas, excepto los datos de salud y los datos relativos a la comisión de infracciones penales o administrativas (art. 7.4 LOPD). Por tanto, hay que entender que, incluso pese a cumplir con los requisitos que a continuación se indicarán, no podrán crearse este tipo de ficheros, si bien resulta bastante confusa la referencia a que la finalidad sea almacenar estos datos[890]. Lo que debe deducirse es que no pueden almacenarse este tipo de datos, con el fin de evitar que, en un futuro, se puedan utilizar para alguna finalidad que aún no está determinada. Esta prohibición adquiere en el mundo de Internet una nueva perspectiva, ya que es posible acumular una gran cantidad de datos. Las posibilidades de utilización de esta información acumulada aumentan, con el nacimiento de nuevos modelos de negocio y nuevas herramientas de análisis de esta información[891].

Los requisitos para tratar estos datos difieren según el tipo de dato. En un primer grupo se incluirían los datos que puedan revelar la ideología, afiliación sindical, religión o creencias. Estos datos tendrían un componente ideológico y, con la excepción de la afiliación sindical tendrían una especial carga de constitucionalidad, en función de la referencia al artículo 16.2 CE, que dispone que nadie pueda ser obligado a declarar sobre su ideología, religión o creencias[892]. Si bien es cierto que la referencia a estos datos también se puede enlazar con el artículo 14 CE que prohíbe toda discriminación por razón de nacimiento, raza, sexo, relación, opinión o cualquier otra circunstancia personal o social.

---

genética (art. 5.1.g) RLOPD). Respecto a los datos biométricos ya había dejado claro el TC que no se entendían incluidos en el régimen de datos especialmente protegidos cuando inadmitió un recurso de amparo en el que se el recurrente atacaba el sistema de control horario mediante lectura de la palma de la mano impuesto por la Administración de la Comunidad Autónoma de Cantabria, ATC 57/2007, de 26 de febrero de 2007, FJ 6.

[890] Algunos autores encuentran el encaje perfecto de este precepto con la limitación de las Fuerzas y Cuerpos de Seguridad de almacenar datos de este tipo, lo que sería una regulación coherente con la limitación que establece el artículo 22.3 LOPD que seguidamente se analizará. M.T. CASADO CADARSO, M.A. VILA MUNTAL, "Los ficheros de las Fuerzas y Cuerpos de Seguridad", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.,* pág. 1.401.

[891] Ver Capítulo VIII.

[892] M.M. SERRANO PÉREZ, *El derecho fundamental a la protección de datos. Derecho español y comparado, op. cit.,* págs. 389 a 392.

Este grupo de datos precisa para su tratamiento, como regla general, la solicitud de consentimiento expreso y por escrito del interesado (art. 7.2 LOPD). Cuando se recoja el consentimiento para tratar estos datos se advertirá al interesado acerca de su derecho a no prestarlo (art. 7.1 LOPD). No obstante, se excepciona del cumplimiento de estos requisitos a los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de datos precisará del consentimiento del afectado (art. 7.2 LOPD)[893].

Otro grupo de datos sería el de los que hagan referencia al origen racial, a la salud y a la vida sexual. Estos sólo podrán ser recabados, tratados y cedidos cuando por razones de interés general, así lo disponga una ley o el afectado consienta expresamente (art. 7.3 LOPD).

Una excepción que se aplicará a ambos grupos de datos es cuando resulte necesario para la prevención o para el diagnóstico médico o la gestión de servicios sanitarios (art. 7.6 LOPD). En este caso se exige que el tratamiento de datos lo realice un profesional sanitario sujeto al secreto profesional u otra persona sujeta a una obligación equivalente de secreto. Este supuesto coincidiría con el establecido por la Directiva 95/46/CE en su artículo 8.3. El GA29 ha insistido en que deben cumplirse los fines indicados en el precepto[894].

Asimismo, también se podrán tratar los datos para salvaguardar el interés vital del afectado o de otra persona, si el afectado está incapacitado para dar su consentimiento. Respecto a esta excepción relativa al interés vital, hay que recordar que también

[893] Excepción que se corresponde con la que establece el artículo 8.2.d) Directiva 95/46/CE, aunque en la directiva se refiere al tratamiento de todas las categorías de datos (origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, los datos relativos a la salud o a la sexualidad).

[894] El GA29 entiende que este supuesto sólo cubriría el tratamiento de datos para el propósito específico de proporcionar servicios relativos a la salud de carácter preventivo, de diagnóstico, terapéutico o de convalecencia, y a afectos de la gestión de estos servicios sanitarios, como por ejemplo, facturación, contabilidad o estadísticas. Quedarían fuera de este supuesto los ejemplos que se indican para poder invocar el artículo 8.4 Directiva 95/46/CE, que veremos se han utilizado en el artículo 8 LOPD. Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), 00323/07/ES WP 131, 15.2.2007, Grupo de trabajo Artículo 29 sobre la protección de datos, págs. 11 a 13.

constituye una excepción a la solicitud de consentimiento, en la regulación general del artículo 6.2 LOPD, por lo que hay que entender que se podrán tratar todo tipo de datos, si es con esa finalidad, sin necesidad del consentimiento del afectado. El GA29 ha indicado que este supuesto sólo debería utilizarse para tratamientos de datos que se realicen en beneficio del interesado, sin poder usarlos, por ejemplo para la investigación médica[895].

Otra excepción que también afecta a los dos grupos de datos es la que se refiere a los ficheros de las Fuerzas y Cuerpos de Seguridad. La LOPD distingue en estos ficheros, entre los que tienen fines administrativos y los que tienen fines policiales[896]. Solo en este último caso se contempla un régimen especial, en el que se permite que puedan tratarse datos sin tener que cumplir con los requisitos que marca el régimen general.

En estos ficheros con fines policiales se podrán tratar datos de carácter personal sin consentimiento de las personas afectadas, aunque deberá limitarse el tratamiento a los datos necesarios para la prevención de un peligro real para la seguridad pública, o para la represión de infracciones penales (art. 22.2 LOPD). Los datos especialmente protegidos, se podrán tratar exclusivamente cuando sea absolutamente necesario para los fines de una investigación concreta[897] y, sin perjuicio del control de legalidad de la actuación administrativa, o de la obligación de resolver las pretensiones formuladas, que corresponden a los órganos jurisdiccionales (art. 22.3 LOPD).

Así como en el caso de los datos de carácter personal normales se menciona que podrán tratarse sin consentimiento para los fines indicados, no se menciona al consentimiento en la habilitación para tratar datos especialmente protegidos. Por lo tanto, cabe plantearse si es preciso solicitar el consentimiento cuando se traten este tipo de

[895] Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), *op. cit.*, pág. 10.

[896] Como recuerda BAYO DELGADO, los datos policiales no entran en el ámbito de aplicación de la Directiva 95/46/CE y fue el legislador español quien soberanamente decidió incluirlos. En cambio, se excluyeron los ficheros establecidos para la investigación del terrorismo y formas graves de delincuencia organizada (art. 2.2.c) LOPD). J. BAYO DELGADO, "Los artículos 22, 23.1 y 24.1 LOPD", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, pág. 1.342.

[897] Por tanto, los datos especialmente protegidos no pueden tratarse para prevenir un peligro, real o hipotético, para la seguridad pública o prevenir hechos delictivos, sino que debe limitarse el tratamiento a cuando la investigación se refiera a un delito concreto ya cometido, y estos datos deben ser indispensables para esa investigación y represión del delito. Fijar esta finalidad fue uno de los puntos más debatidos en el la tramitación parlamentaria de este precepto. M.T. CASADO CADARSO, M.A. VILA MUNTAL, "Los ficheros de las Fuerzas y Cuerpos de Seguridad", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, pág. 1.400.

datos, de acuerdo con lo preceptuado en el artículo 7 LOPD. De esta forma, lo que hallaríamos, en esta disposición del artículo 22 LOPD, es solo una limitación a la finalidad del tratamiento. Esta interpretación no parece lógica, ya que imposibilitaría la investigación y no habría suscitado en el trámite parlamentario la necesidad de reforzar la protección, mediante la garantía introducida relativa al control de legalidad y jurisdiccional[898].

Únicamente respecto a los datos relativos a la salud, hay que mencionar una especial legitimación para las instituciones y los centros sanitarios públicos y privados, así como para los profesionales sanitarios, que podrán tratar estos datos de las personas que acudan o deban ser tratados, de acuerdo con lo previsto en la legislación estatal o autonómica sobre sanidad (art. 8 LOPD)[899]. Por tanto, la LOPD se remite, en este caso, a la legislación sectorial relativa a la sanidad, ya que esta normativa regula específicamente cómo se debe tratar esta información, parte esencial del servicio médico. Este precepto hallaría su origen en la posibilidad que otorga la Directiva 95/46/CE a los Estados miembros de establecer excepciones a la prohibición general de tratar este tipo de datos especialmente protegidos (art. 8.4 Directiva 95/46/CE)[900].

Sorprende que se establezcan aparentemente dos regulaciones dirigidas a los servicios sanitarios. En la primera (art. 7.6 LOPD) se podrán tratar todo tipo de datos y en la segunda (art. 8 LOPD) se enfoca únicamente a los de salud. Hay que entender que en este segundo caso, al ser consecuencia de la utilización por parte de nuestro legislador de

[898] SERRANO PÉREZ alude a este defecto en el texto del artículo 22 LOPD y estima que se podría excluir el consentimiento respecto a los datos del artículo 7.3 LOPD pero no respecto a los del artículo 7.2 LOPD, ya que esto llevaría a la inconstitucionalidad del precepto por no respetar el artículo 16.3 CE. M.M. SERRANO PÉREZ, *El derecho fundamental a la protección de datos. Derecho español y comparado*, *op. cit.*, págs. 400 a 404. También alude a esta problemática P. NICOLAS JIMÉNEZ, "Ficheros policiales de perfiles de ADN", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, *op. cit.*, pág. 1.438.

[899] Como indica SERRANO PÉREZ no se trata de un reenvío a un régimen que estaría al margen de la LOPD, sino que es más un reconocimiento de la LOPD por las garantías y derechos contemplados en estas leyes específicas M.M. SERRANO PÉREZ, *El derecho fundamental a la protección de datos. Derecho español y comparado*, *op. cit.*, pág. 410.

[900] El Considerando 34 Directiva 95/46/CE menciona como posibles sectores en los que se podrá utilizar esta posibilidad los de la salud pública y la protección social, particularmente en lo relativo a la garantía de la calidad y la rentabilidad, así como en los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, la investigación científica y las estadísticas públicas.

una excepción que permite la Directiva 95/46/CE, en su artículo 8.4, por motivos de interés público importantes, se haya restringido el tipo de datos a los que se extiende[901].

Los datos relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras. Esta previsión que transpone el artículo 8.5 Directiva 95/46/CE no contempla ninguna excepción, lo que permitía la directiva. En el caso de la LOPD no se ha previsto, por tanto, el posible tratamiento de este tipo de datos por entidades que habitualmente deben utilizarlos y no son administraciones públicas, como sucede, por ejemplo, con los abogados[902].

Hay que destacar que algunos supuestos que establece la Directiva 95/46/CE, que permiten excepcionar la prohibición de tratamiento de este tipo de datos especialmente protegidos, no se contemplan en la LOPD. Así, no se incluye la posibilidad de tratar datos de este tipo para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de derecho laboral, en la medida en que esté autorizado por la legislación y ésta prevea las garantías adecuadas, y la de tratar datos, que el interesado haya hecho manifiestamente públicos, o el que permite tratar estos datos, cuando sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial (art. 8.2.b) y e) Directiva 95/46/CE).

Tampoco se ha previsto nada en la LOPD sobre lo que dispone el artículo 8.7 Directiva 95/46/CE con relación al número nacional de identificación, lo que, sin duda, se debe a que, en España, el tratamiento de este dato no supone ningún problema, ya que tenemos una larga tradición en la utilización del documento nacional de identidad. Por eso, hay que acudir a la regulación sectorial referente a este documento para hallar los criterios que se han fijado para el tratamiento de los datos que allí se contienen, que

[901] Sin embargo, SERRANO PÉREZ entiende que el artículo 8 se refiere al uso de los datos en el terreno sanitario con una finalidad asistencial y para ello establece un régimen particular y el artículo 7 contempla un régimen al margen del ámbito sanitario, por ejemplo el ámbito laboral o la educación. M.M. SERRANO PÉREZ, *El derecho fundamental a la protección de datos. Derecho español y comparado*, *op. cit.*, págs. 414 a 415.

[902] Hay que recordar que algunas legislaciones nacionales europeas sí han tenido en cuenta estos supuestos, como el artículo 12.1.11 Ley finlandesa que ha previsto que puedan tratar este tipo de datos los abogados o las compañías de seguros.

incluyen datos biométricos y datos de certificados digitales que permiten firmar electrónicamente al ciudadano para identificarse en tramitaciones digitales[903].

2.3. La obligación de informar

2.3.1. La información como elemento del contenido esencial del derecho de protección de datos

Como indicó el TC, el derecho a la protección de datos garantiza a los individuos un poder de disposición sobre sus datos. Pero para que sea efectiva esa garantía, el individuo debe conocer los datos que poseen los terceros, quiénes son estos terceros y con qué fin los poseen[904]. Este derecho a saber y ser informado, especialmente, de quién tiene los datos y para qué los utiliza forma parte del haz de facultades que se atribuye a los titulares del derecho a la protección de datos y que conforma el contenido esencial de este derecho[905]. El incumplimiento del deber de informar conllevará, por tanto, una vulneración del derecho fundamental a la protección de datos.

Así lo consideró el Alto Tribunal en STC 29/2013, de 11 de febrero de 2013, en la que estimó vulnerado, por la Universidad de Sevilla, el contenido esencial del derecho a la protección de datos de uno de sus funcionarios, al no cumplirse con este derecho de información. La Universidad de Sevilla lo había sancionado por faltas de puntualidad, transgresión de la buena fe contractual y abuso de confianza. Este funcionario debía cumplimentar unas hojas de control de asistencia indicando la hora de entrada y la de salida. La Universidad comprobó que las horas que indicaba el trabajador no eran reales, comprobación que pudo llevar a cabo la Universidad, mediante el acceso al sistema de

[903] Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
[904] STC 292/2000 de 30 de noviembre de 2000, FJ 6.
[905] Si bien DÍAZ REVORIO estimaba que el TC en esta STC 292/2000 no manifestaba claramente que la información formara parte del contenido esencial del derecho, concluye que la información es imprescindible para otorgar el consentimiento, por lo puede entenderse como elemento del contenido esencial. F.J. DÍAZ REVORIO, "Derecho de la información en la recogida de datos. Una perspectiva constitucional", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, págs. 436 a 437. Por el contrario, no albergaban dudas R. MARTÍNEZ MARTÍNEZ, "Menores y redes sociales. Condiciones para el cumplimiento del artículo 13 del Reglamento de desarrollo de la Ley Orgánica de protección de datos", A. RALLO LOMBARTE, R. MARTÍNEZ MARTÍNEZ (Ed.) VVAA, *Derecho y redes sociales, op. cit.*, pág. 221, o M.V. GUERRERO PICÓ, *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal, op. cit.*, pág. 250 o A. TRONCOSO REIGADA, *La protección de datos personales. En busca del equilibrio, op. cit.*, págs. 456 a 457.

videovigilancia que tenía instalado en los accesos a la facultad donde se encontraba el funcionario.

El trabajador acudió a los tribunales para impugnar estas sanciones pero, tanto el Juzgado de lo Social núm. 3 de Sevilla, como el Tribunal Superior de Justicia de Sevilla al que se acudió en suplicación, entendieron que el uso de la videovigilancia había respetado el principio de proporcionalidad exigido por la doctrina para poder imponer una medida restrictiva de los derechos fundamentales[906]. El Tribunal Constitucional se refirió a la STC 292/2000, de 30 de noviembre de 2000, que incluía este derecho de información en el núcleo esencial del derecho a la protección de datos, y consideró que no se había cumplido con el mismo con la existencia de distintivos que anunciaban la instalación de cámaras y captación de imágenes, por lo que anuló las sanciones. El TC estimó que:

> "era necesaria además la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida. Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo." STC 29/2013, FJ 8

El Tribunal Supremo también se ha manifestado sobre la relevancia de la información en una sentencia donde desestima un recurso de casación para la unificación de doctrina[907]. Un supermercado había despedido a una cajera por no cobrar algunos productos a un cliente, expareja de la empleada. La empresa utilizó el sistema de videovigilancia, instalado tres años antes como prueba de este hecho que supuso la sanción consistente en el despido de la trabajadora. Ésta denunció los hechos, al entender que no había sido informada de la finalidad de control de la actividad laboral y, por lo tanto, al haberse utilizado una prueba obtenida ilícitamente, al vulnerar el derecho de protección de datos[908]. Estos argumentos fueron corroborados por la sentencia de instancia que había declarado la nulidad el despido y por el Tribunal Superior de Justicia del País Vasco.

---

[906] De nada sirvió que el trabajador aportara en segunda instancia la resolución de la AEPD, que consideraba que la Universidad no había cumplido con el deber de informar a los trabajadores sobre el uso relativo al control horario que se iba a realizar con las imágenes del sistema de videovigilancia. STC 29/2013, de 11 de febrero de 2013, FFJJ 6, 7 y 8.

[907] STS de 13 de mayo de 2014 (Sala 4ª) (ROJ: STS 2618/2014)

[908] *Ibídem*, FJ 1.

La información que se había proporcionado en el momento de instalación de las cámaras a la representante de los trabajadores había sido que el sistema de vigilancia no estaba destinado al control laboral, sino a evitar robos por terceros y que algunas de las cámaras ni siquiera estarían operativas[909]. El Tribunal Supremo tuvo en cuenta el carácter permanente del sistema de videovigilancia y la información proporcionada que contradecía directamente la utilización realizada y desestimó el recurso de la empresa[910].

Hay que mencionar un voto particular a esta sentencia, que plantea una interesante reflexión, al entender que la protección de los derechos fundamentales no puede ir más allá de lo razonable y no puede proteger a los autores de hechos ilícitos si su acción ha sido advertida por un control causal, por cámaras a la vista, que conoce el autor, aunque no se le haya advertido[911]. Se pregunta el Magistrado "¿Qué pasa con los hallazgos casuales? ¿Qué sucede si la cámara visiona en la cola de la caja un homicidio, un acoso sexual y otro delito cometido por un empleado? ¿Estaremos ante una prueba ilícita y el acosador y homicida serán absueltos?". Independientemente del caso concreto, hay que enfatizar la dificultad del equilibrio de la protección de los diversos derechos, equilibrio que, en un primer momento, debe hallar el responsable y que, posteriormente, ante el conflicto, deberán hallar las autoridades de protección de datos y los órganos judiciales.

Otra característica del derecho la información, es que se configura como un derecho instrumental para permitir que el interesado pueda consentir sobre la recogida y uso de sus datos personales[912]. Por eso, en caso de que el supuesto que legitima el

[909] *Ibídem*, FJ 6.
[910] *Ibídem.* La STC 186/2000, de 10 de julio, alegada fue muy similar al caso planteado ya que también se habían instalado cámaras para grabar a una cajera de un supermercado sobre la que habían sospechas de que cometía irregularidades. Sin embargo en esta sentencia se había alegado la vulneración del derecho a la intimidad y las cámaras se instalaron de forma puntual.
[911] Para ilustrar sus argumentos el Magistrado que emite el voto particular, D. José Manuel López García de la Serrana, menciona una sentencia del TEDH, en la que se planteó el caso de un abogado sevillano que había sido grabado, sin su consentimiento, mientras conducía una motocicleta por las calles de Sevilla, durante varios días. La grabación la realizaron unos detectives privados contratados por una compañía de seguros que presentó el vídeo como prueba en un procedimiento civil contra el abogado, porque éste alegaba, que en un accidente sufrido con el asegurado de la compañía había sufrido daños psicológicos que le impedían conducir ningún vehículo. El TEDH estimó que la injerencia en el derecho a la vida privada del artículo 8 CEDH fue proporcionada, ya que no se grabó de forma permanente sino puntual, no se pretendía difundir las imágenes sino utilizarlas en el marco de un juicio y la grabación se realizó en la vía pública por detectives, de acuerdo con exigencias legales. Sentencia del TEDH de 27 de agosto de 2014, *La Flor Cabrera c. Espagne*, apdos. 35, 38-40.
[912] "En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a

tratamiento de datos fuera el del consentimiento del interesado, deberá cumplirse con este derecho a ser informado que deberá adaptarse a los requisitos exigidos para que el consentimiento sea válido.

Pese a esta conexión con el consentimiento, hay que tener presente que el derecho a ser informado tiene un carácter autónomo con relación a los otros derechos y principios que garantiza este derecho. Por tanto, es un derecho independiente de la legitimación que deba tener el responsable para poder tratar los datos. De esta forma, y sin perjuicio de las excepciones al cumplimiento del derecho que luego se abordarán, sea cual sea el supuesto que permite al responsable tratar los datos, deberá cumplirse con el deber de informar[913].

2.3.2. Requisitos de la obligación de informar

Pese a que el artículo 5 LOPD se titula "Derecho de información en la recogida de datos", el contenido de este precepto se dirige claramente al responsable, al establecerse desde la perspectiva de lo que "debe" cumplir éste, como sucede de forma generalizada en la LOPD[914]. En esta rúbrica también queda claro que la obligación se refiere a la fase inicial del ciclo del tratamiento[915]. El régimen general del derecho de información que

saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele", STC 292/2000, FJ 7.

[913] Lo confirma el Tribunal Constitucional que entiende que: "[…] se confundiría la legitimidad del fin (en este caso, la verificación del cumplimiento de las obligaciones laborales a través del tratamiento de datos, art. 20.3 LET en relación con el art. 6.2 LOPD) con la constitucionalidad del acto (que exige ofrecer previamente la información necesaria, art. 5 LOPD), cuando lo cierto es que cabe proclamar la legitimidad de aquel propósito (incluso sin consentimiento del trabajador, art. 6.2 LOPD) pero, del mismo modo, declarar que lesiona el art. 18.4 CE la utilización para llevarlo a cabo de medios encubiertos que niegan al trabajador la información exigible." STC 29/2013, FJ 7.

[914] Como indica DÍAZ REVORIO, el artículo 5 LOPD "a pesar de su denominación, olvida su vertiente como derecho" y gráficamente lo califica este autor como un "derecho-deber". F.J. DÍAZ REVORIO, "Derecho de la información en la recogida de datos. Una perspectiva constitucional", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, *op. cit.*, págs. 439, 450.

[915] Hay que tener en cuenta que la regulación separada de la fase de recogida proviene de la primera Propuesta de Directiva de 1990 (art. 13 Propuesta de Directiva de 1990 que se refería a la "Información en el momento de la recogida de datos"), que sirvió de inspiración para la elaboración de la LORTAD y que así se ha mantenido hasta la LOPD. Sin embargo en la versión final de la Directiva 95/46/CE se optó por una regulación unitaria de todas las operaciones de tratamiento y en los artículos 10 y 11 se evitó la referencia a la recogida, realizándose de forma más neutra una referencia a recabar datos.

tienen los interesados se incluye en el artículo 5 LOPD. No obstante, la LOPD contiene también algunas especialidades en el contexto de los ficheros privados[916].

Así como la Directiva 95/46/CE no contiene ninguna referencia al modo en que debe cumplirse con esta obligación, la LOPD especifica que, en caso de que los datos se recojan directamente de los interesados, éstos deben ser previamente informados de modo expreso, preciso e inequívoco. Por lo tanto, se trata de una obligación con unas características que la revisten de un gran rigor (previa a recoger los datos, realizada de modo expreso, preciso e inequívoco). En suma estos requisitos implican que el interesado no puede tener dudas acerca de esta información que se le proporciona.

Si se utilizan cuestionarios u otros impresos para la recogida de los datos, se obliga a que figure en los mismos, en forma claramente legible, el contenido de la información que se especifica en el primer apartado del artículo 5 (art. 5.2 LOPD). Por tanto, rige la libertad de forma para el cumplimiento de esta obligación[917]. En el contexto de la videovigilancia, la AEPD y la ACPD han elaborado unos modelos de cartel mediante los que se proporciona la información esencial relativa a la identidad del responsable y la dirección para ejercer los derechos. De esta forma, se adapta el cumplimiento de esta obligación al entorno. Para completar el contenido que exige el

[916] Así, además de la regulación de la excepción que el mismo artículo 5.5 LOPD establece respecto a las actividades de publicidad o prospección comercial (arts. 30.2 LOPD y 45.2 RLOPD) también se contemplan especiales deberes de información para los ficheros de información sobre solvencia patrimonial y crédito (arts. 29.2 LOPD, 39 y 40 RLOPD).

[917] Así lo confirmó el Tribunal Supremo mediante sus SSTS de 15 de julio de 2010 (Sala 3ª) (ROJ: STS 4050/2010), FJ 9 y de 15 de julio de 2010 (Sala 3ª) (ROJ: STS 4057/2010), FJ 10 que remite al FJ 9 de la otra sentencia, mediante las que anuló el artículo 18 RLOPD que establecía: "El deber de información al que se refiere el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado. El responsable del fichero o tratamiento deberá conservar el soporte en el que conste el cumplimiento del deber de informar. Para el almacenamiento de los soportes, el responsable del fichero o tratamiento podrá utilizar medios informáticos o telemáticos. En particular podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales". El precepto, según el Tribunal suponía el establecimiento de una nueva obligación con respecto a lo que se establece en la LOPD: la obligación de que la prueba del efectivo cumplimiento constase documentalmente o por medios informáticos o telemáticos, lo que podría inducir a que se apreciara un cierto grado de desconfianza respecto a la conducta de quienes pudiendo preconstituir, sin grandes dificultades apreciables, un medio probatorio hicieran caso omiso a la exigencia. El Tribunal Supremo indica que el artículo 5 LOPD no establece ninguna previsión acerca de la forma en la que debe cumplirse con el deber de informar y la referencia que realiza en su apartado 2 a la posibilidad de utilizar cuestionarios o impresos para la recogida de datos sólo se hace para establecer la obligación de que incluyan el contenido de la información, no para obligar a que se realice mediante este tipo de documentos. Por ello, concluye el Tribunal que debe considerarse que el legislador ha optado por la libertad de forma.

artículo 5 LOPD, el responsable deberá tener a disposición de los interesados la cláusula informativa con la información completa[918].

2.3.3. Información en el caso de que los datos se obtengan directamente del interesado

Como se pudo ver, al analizar esta obligación en la Directiva 95/46/CE, se diferenciaban dos bloques de información, según si los Estados miembros debían incluirlos como contenido obligatorio o, por el contrario, se trataba de un contenido opcional. La LOPD respeta el contenido obligatorio que contempla la Directiva 95/46/CE en la recogida directa, aunque con algunos matices y contenido adicional.

> "1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos. d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. (…) 3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban." (art. 5.1 y .3 LOPD)

Si bien se respeta el hecho de tener que informar sobre la finalidad, esta va referida a la recogida de los datos, no al tratamiento, como sucede en la Directiva 95/46/CE. La recogida es sólo una fase del tratamiento de datos y, por tanto, no sería correcto informar sólo de la finalidad que se pretende con esta fase, sino la finalidad que se persigue con todo el tratamiento. Sin duda hay que interpretar así este aspecto.

El contenido adicional que se añade en la LOPD es la información sobre la existencia del fichero o tratamiento de datos y sobre los destinatarios de la información. Tener que informar de la existencia del fichero o tratamiento parece superfluo. No obstante, podría tener una trascendencia para el interesado porque obligaría a clarificar si los datos se destinarán a un tratamiento o a un fichero. Si los datos se destinan a un tratamiento significa que el responsable no tiene obligación de notificarlo a la AEPD y no

[918] Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, BOE núm. 296, 12.12.2006, págs. 43458-43460 e Instrucción 1/2009, de 10 de febrero, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia, DOGC, núm. 5322, 19.2.2009, págs. 13258-13272.

se dará publicidad del mismo en el Registro General de Protección de Datos. Por tanto, es más importante, si cabe, que el interesado conozca la información que se le proporcione al respecto.

El otro aspecto que la LOPD introduce en el bloque obligatorio es el de los destinatarios de la información[919]. En la LOPD no se incluía la definición de destinatarios, pero se incorporó en el RLOPD: "Destinatario(o cesionario): persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos. Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados" (art. 5.1.h) RLOPD).

En la Directiva 95/46/CE, el destinatario era cualquier sujeto que pudiera recibir una comunicación de datos, incluso las personas bajo la autoridad directa del responsable[920]. En virtud del contenido de la definición del RLOPD se podría interpretar que también cabrían en esta figura las personas bajo la autoridad del responsable. La definición de cesión que es "tratamiento de datos que supone su revelación a una persona distinta al interesado" (art. 5.1.c) RLOPD), tampoco contradice que el destinatario o cesionario pueda ser, por ejemplo, un empleado del responsable. Sin embargo, se ha interpretado que la cesión es a sujetos diferenciados del responsable, pese a que puedan no tener personalidad jurídica, como establece la definición (por ejemplo, un comité de empresa de la empresa responsable[921] o un socio de la asociación responsable[922]). Lo que caracterizará al cesionario es que no tendrá una relación de dependencia del responsable.

Esta postura se confirma con la interpretación adoptada en la regulación del derecho de acceso que, entre otros aspectos, obliga a informar de los cesionarios de datos (art. 29.3 in fine RLOPD). En algunas ocasiones el interesado ha solicitado que se le informase de aquellos empleados o usuarios del sistema informático que hubieran accedido a los datos. Tanto la Audiencia Nacional, como la AEPD, han interpretado que

[919] La referencia a "destinatarios de la información" para ser más correcta debería ser a "destinatarios de los datos", como establece la Directiva 95/46/CE. Además de que se añade este aspecto adicional, que de por sí ya es un plus en los requisitos a cumplir, se hace de forma más restrictiva si cabe, ya que la Directiva 95/46/CE permitía elegir entre informar de los destinatarios o informar de las categorías de destinatarios, lo que constituye un deber más laxo.
[920] Ver Capítulo V.
[921] Informe 0488/2009 de la AEPD.
[922] Informe 0645/2009 de la AEPD.

no debía proporcionarse esta información, si bien es cierto que no se profundizaba en la problemática apuntada respecto a la definición de destinatario[923]. En conclusión, hay que entender que el término "destinatarios", en este artículo 5 LOPD responde a los cesionarios, que serán sujetos que no estén bajo la autoridad del responsable, por lo que sería contrario a la definición que realiza la Directiva 95/46/CE de "destinatario"[924].

En lo referente al bloque de información opcional, la LOPD incorpora todos los ejemplos que citaba la Directiva 95/46/CE (uno de ellos, como se ha indicado, incluido en el bloque obligatorio). En la LOPD se establece que esta información no será necesaria, si su contenido se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban[925]. Esto no es exactamente lo que precisa la Directiva 95/46/CE que se centra en las circunstancias específicas en las que se obtienen los datos para valorar si esta información suplementaria resulta necesaria para garantizar un tratamiento de datos leal respecto del interesado. Por tanto, la Directiva 95/46/CE ofrece un criterio (las circunstancias en las que se obtienen los datos), pero lo que hay que perseguir es que se garantice con esa información que el tratamiento de datos sea leal.

[923] De hecho, la Audiencia Nacional incluso hace referencia a la regulación del derecho de acceso de la Directiva 95/46/CE, sin tener en cuenta que en ésta se menciona a los destinatarios y ya se ha indicado que la definición de destinatario sí incluiría a las personas autorizadas por el responsable a acceder a los datos. Aunque también es cierto que la Directiva 95/46/CE considera esta información opcional. SAN de 4 de marzo de 2013 (Sala de lo contencioso-administrativo) (ROJ: SAN 971/2013), FJ 4 e Informe 0167/2005 de la AEPD.

[924] Ver Capítulo V. No coincido con APARICIO SALOM, que entiende que el "destinatario" que aparece mencionado en el artículo 5.1.a) LOPD no se refiere a las cesiones sino al supuesto en el que la obtención de datos no se realice directamente por el responsable del tratamiento, sino por un tercero fruto de un encargo. En cambio, sí estoy de acuerdo con el autor que afirma que es absurdo que el inciso segundo del artículo 5.1.e) LOPD establezca una obligación de organización en el seno del artículo 5 que está dedicado a regular la obligación de informar, cuando regula la necesidad de que el responsable no establecido en la UE designe un representante en España. Se deduce que se hace porque se debe informar de quién es el representante pero no debería incluirse aquí la obligación de nombrarlo sino sólo la de informar sobre su existencia. J. APARICIO SALOM, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, 4ª ed., *op. cit.*, págs. 211 a 212. También opina mismo respecto al representante M.V. GUERRERO PICÓ, *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, *op. cit.*, pág. 253.

[925] DÍAZ REVORIO considera que, al exigir que el contenido de la información se deduzca de la naturaleza de los datos o de las circunstancias en que se recaban, no es una excepción al contenido de la información que se ha de transmitir, sino que se refiere a la manera en que la misma es expresada y transmitida. Lo que se excepcionaría es el requisito de que la información se transmita de forma expesa. F.J. DÍAZ REVORIO, "Derecho de la información en la recogida de datos. Una perspectiva constitucional", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, *op. cit.*, pág. 444.

Los aspectos que forman este bloque de información opcional son: el carácter obligatorio o facultativo de la respuesta a las preguntas que se planteen (en este caso, se añade en la LOPD a lo que establece la Directiva 95/46/CE: "a las preguntas que se planteen"); las consecuencias de la obtención de los datos o de la negativa a suministrarlos (se añade en la LOPD "de la obtención de los datos"); la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición (se añade "cancelación y oposición").

Hay que hacer mención a la excepción en la aplicación de esta regulación recogida en el artículo 5, apartados 1 y 2, que se ha establecido para los ficheros de titularidad pública. No será aplicable esta regulación cuando la información afecte a la defensa nacional, a la seguridad pública o a la persecución de infracciones penales (art. 24.1 LOPD). Así se acogería esta disposición a la posibilidad que brinda la Directiva 95/46/CE de establecer excepciones al alcance de este derecho de información (art. 13 Directiva 95/46/CE). La excepción tuvo que ser recortada por el Tribunal Constitucional en la STC 292/2000, de 30 de noviembre de 2000[926].

2.3.4. Información en el caso de que los datos no se obtengan directamente del interesado

En caso de que los datos no procedan del mismo interesado se debe informar a éste de forma expresa, precisa e inequívoca, en un plazo de tres meses a contar desde que se registran los datos, salvo que ya hubiera sido informado con anterioridad: del contenido del tratamiento, de la procedencia de los datos, de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información, de la posibilidad de ejercitar los derechos de acceso,

[926] El artículo 24.1 LOPD establecía en su redacción original que: "lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información del afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las administraciones públicas o cuando afecte a la defensa nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas"(el subrayado es de la autora para señalar los aspectos declarados insconstitucionales y nulos por el TC). El Tribunal Constitucional señaló que la LOPD, al incluir los aspectos subrayados, lo que hacía era apoderar a la administración pública para fijar los límites a este derecho a ser informado, de forma que dejaba en la incertidumbre al ciudadano sobre los casos en que podría concurrir esta circunstancia, sino en todos, en virtud de lo amplio de las expresiones "funciones de control y verificación" o la afectación a infracciones administrativas. Esto supondría el traslado por parte del legislador a la administración del desempeño de una función que sólo le compete a él mismo, como es el establecimiento de los límites a los derechos fundamentales, de acuerdo con la reserva de ley del artículo 53.1 CE. STC 292/2000, FFJJ 16, 17.

rectificación, cancelación y oposición y de la identidad y dirección del responsable del tratamiento, o en su caso, del representante (art. 5.4 LOPD).

Lo primero que hay que resaltar con relación a la regulación de la Directiva 95/46/CE es que se han eliminado de esta regulación de la LOPD las opciones en cuanto al momento en el que se debe cumplir con la obligación de información. En la Directiva 95/46/CE se establecían dos opciones: desde el momento del registro o cuando se piense comunicar los datos a un tercero, a más tardar en el momento de la primera comunicación de datos (art. 11.1 Directiva 95/46/CE). En la LOPD no se permite optar por estos dos momentos, sino que se obliga a informar en un plazo de tres meses desde el registro de los datos, independientemente de que se prevea o no una comunicación de datos.

En segundo lugar, no hay información opcional en la LOPD, toda la información es obligatoria y además ésta es más amplia que la que menciona la Directiva 95/46/CE[927].

Se establecen varias excepciones a esta obligación de información a los interesados cuando sus datos no proceden directamente de ellos, acordes con la Directiva 95/46/CE, aunque hay que matizar alguna diferencia. Si la Directiva 95/46/CE se refiere como posible excepción a que el registro o la comunicación de datos a un tercero estén expresamente prescritos por ley (art. 11.2 Directiva 95/46/CE), la LOPD lo que indica es que no se aplicará el régimen general "cuando expresamente una ley lo prevea" (art. 5.5 LOPD).

De la literalidad del precepto de la LOPD se extrae que, para que no deba cumplirse con este deber de informar debería constar esta excepción expresamente en la ley, lo que no sería muy factible, por lo que debería interpretarse esta disposición, de acuerdo con lo que indica la Directiva 95/46/CE, de forma que si lo que establece la ley expresamente es que se realice el registro de los datos o la comunicación de los mismos,

[927] Hay que entender que, cuando la LOPD menciona "el contenido del tratamiento", esta información debe equipararse con la que menciona la Directiva 95/46/CE como información adicional y que se refiere a las categorías de los datos de que se trate. Como información que no se establece en la Directiva 95/46/CE, ni siquiera como información adicional, está la procedencia de los datos, la existencia de un fichero o tratamiento de datos de carácter personal y la posibilidad de ejercitar los derechos de cancelación y oposición.

entonces quede excepcionado este deber de informar, ya que éste se garantizará mediante una disposición legal[928].

Los otros presupuestos que establece el artículo 5.5 LOPD son: cuando el tratamiento tenga fines históricos, estadísticos o científicos o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados. Respecto a este último supuesto, se ha establecido como garantía que sea la AEPD o el organismo autonómico equivalente quien decida si puede aplicarse la excepción. Se incluyen los criterios que las agencias podrán tener en cuenta: el número de interesados, la antigüedad de los datos y las posibles medidas compensatorias[929]. También se excepciona la obligación de informar cuando los datos procedan de datos de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial. En este caso, se incluye una obligación de informar en cada comunicación que se dirija al interesado del origen de los datos, de la identidad del responsable del tratamiento y de los derechos que le asisten.

Por último, hay que hacer referencia a un supuesto especial regulado en el RLOPD, en el que se ha aclarado que no se entenderá que hay cesión cuando se produce una modificación en el responsable como consecuencia de operaciones mercantiles de reestructuración societaria (art. 19 RLOPD). En este caso se especifica que deberá cumplirse con lo previsto en el artículo 5 LOPD.

2.4. La obligación de notificación a la autoridad de control

Respecto a esta obligación de notificación a la autoridad de control hay que destacar dos aspectos que caracterizan la regulación española: el establecimiento de un derecho de los interesados a consultar el Registro General de Protección de Datos (art. 14

[928] Así lo ha entendido también la AEPD, si bien precisa que la aplicación de esta excepción se producirá en supuestos "en que el tratamiento o cesión de los datos de carácter personal aparece recogido expresamente en una norma con rango de Ley, pero no a aquellos supuestos en que la Ley "autorice" o "habilite" la cesión de los datos, pero no la recoja de modo expreso y taxativo en su articulado, sin perjuicio de que en dichos supuestos la cesión se encontrará amparada por lo dispuesto en los artículos 6.2 u 11.2.a) de la Ley Orgánica 15/1999." Informe 60/2004 de la AEPD. DÍAZ REVORIO entiende que las excepciones que se establecen en caso de recogida indirecta al deber de informar, deben analizarse a la luz del derecho fundamental para verificar su conformidad constitucioinal. F.J. DÍAZ REVORIO, "Derecho de la información en la recogida de datos. Una perspectiva constitucional", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, págs. 446 a 447.

[929] La regulación del procedimiento para solicitar esta exención del deber de información se realizará de acuerdo con lo establecido en el RLOPD (arts. 153 a 156 RLOPD).

LOPD) [930] y un régimen diferente relativo a la obligación, según se trate de ficheros de titularidad pública o ficheros de titularidad privada[931].

Respecto a los ficheros de titularidad privada, ya se indicó, al examinar la legitimación para tratar datos, que se establece la posibilidad que tienen las personas, empresas o entidades titulares de crearlos, cuando esto resulte necesario para el logro de su actividad u objeto legítimos y se respeten las garantías que establece la LOPD (art. 25 LOPD). Cuando el responsable decida crear un fichero de titularidad privada deberá notificarlo previamente a la AEPD (arts. 26.1 LOPD y 55.2 RLOPD).

Respecto a los ficheros de titularidad pública, se establece que la creación, modificación o supresión sólo podrá realizarse mediante la publicación de una disposición general o acuerdo en el Boletín Oficial del Estado o el diario oficial correspondiente (art. 20.1 LOPD)[932]. Esta publicación debe ser con carácter previo a la creación, modificación o supresión del fichero (art. 52.2 RLOPD). Tras esta publicación, en un plazo de treinta días, el fichero será notificado a la AEPD para su inscripción en el Registro General de Protección de Datos (art. 55.1 RLOPD).

El RLOPD introdujo un precepto para aclarar la forma que debían revestir las disposiciones generales e introdujo la posibilidad de adoptar un acuerdo (art. 53 RLOPD)[933]. El acuerdo permitía que órganos que no disponían de capacidad reglamentaria, como son las corporaciones de derecho público, pudieran aprobar la

[930] El artículo 14 LOPD establece que "cualquier persona podrá conocer, recabando a tal fin al información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita."

[931] Ver Capítulo III.

[932] La naturaleza de la disposición de carácter general que debía dictarse por el órgano administrativo fue un punto que originó no pocos problemas y, por ello, en el RLOPD se recogieron algunas pautas para determinar el tipo de disposición que debía ser aprobada (art. 53 RLOPD).

[933] La Ley catalana ya había establecido, en su Disposición Final tercera, la forma que debían revestir las disposiciones: "1. Los consejeros de la Generalidad, dentro del ámbito de sus respectivas competencias, quedan habilitados para crear, modificar y suprimir, mediante orden, los ficheros de sus departamentos o de los entes públicos vinculados a ellos o que dependan de los mismos y los ficheros de los consorcios en que la representación de la Administración de la Generalidad en los órganos de gobierno sea mayoritaria. 2. Las entidades de derecho público dotadas de especial independencia o autonomía quedan habilitadas para ejercer la competencia de crear, modificar y suprimir ficheros." También emitió la Recomendación 1/2011 de la *Autoritat Catalana de Protecció de Dades* sobre la creación, modificación y supresión de ficheros de datos de carácter personal de titularidad pública. La Ley vasca dispone en su artículo 4 que la creación, modificación y supresión de ficheros de la Administración de la Comunidad Autónoma se realizará por orden del titular del departamento al que esté adscrito el fichero y en ficheros de otras administraciones, instituciones o corporaciones, ya se permitía que se hiciera mediante disposición o acuerdo.

disposición mediante un acto administrativo, lo que ha sido criticado por algún autor[934]. Para paliar los efectos de la falta de publicidad se establece la necesidad de que el acuerdo se publique en el boletín oficial correspondiente (art. 53.4 RLOPD).

Para los dos tipos de ficheros se establece la necesidad de que el contenido de la inscripción en el registro se mantenga actualizado. Por ello, se establece la obligación que tiene el responsable de notificar las modificaciones y la supresión de los ficheros (art. 58 RLOPD). La legislación española contempla la notificación de ficheros, sin diferenciar el sistema de tratamiento utilizado, automatizado o no automatizado (art. 56.1 RLOPD)[935]. Si el fichero tiene varios responsables, se obliga a cada uno de ellos a notificar el fichero (art. 57 RLOPD).

La AEPD ha establecido dos sistemas para realizar la notificación de los ficheros: el sistema NOTA que sirve para notificar ficheros de titularidad privada y de titularidad pública y el sistema DISPONE que sirve para notificar ficheros de titularidad pública.

No se han acogido en la legislación española las posibilidades que otorgaba la Directiva 95/46/CE de simplificación o exención de la obligación de notificación (art. 18 Directiva 95/46/CE), por lo que no se ha adoptado la figura del encargado de protección de datos. Tampoco se han establecido controles previos para tratamientos que supongan riesgos específicos para los derechos y libertades de los interesados (art. 20 Directiva 95/46/CE). No obstante, aunque no se puede decir que se trate de estos controles establecidos por la Directiva 95/46/CE, se ha previsto la cooperación de la AEPD mediante informes preceptivos en la elaboración de normas que desarrollen la LOPD y de normas que incidan en la protección de datos[936].

2.4.1. El contenido de la notificación

[934] Á. IGUALADA MENOR, "Creación, modificación o supresión de ficheros de titularidad pública", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*,*op. cit.*, págs. 1.289 a 1.290.

[935] Además permite que se realice una única notificación cuando los datos estén almacenados en diferentes soportes, automatizados o no automatizados o se haga, por ejemplo, una copia en soporte no automatizado de un fichero automatizado (art. 56.2 RLOPD).

[936] Así se ha establecido en el artículo 5 Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos (BOE núm. 106 de 4.5.1993).

En referencia a los ficheros de titularidad pública, el contenido que debe precisar la disposición general es similar al que establece el artículo 19 Directiva 95/46/CE con sólo algunas diferencias. En la legislación española se incluye: la identificación del fichero o tratamiento; en lugar de los objetivos del tratamiento, contemplados en la Directiva 95/46/CE se hace referencia a la finalidad y usos previstos; se incluye bastante información acerca del origen de los datos, como el procedimiento de recogida de los datos y su procedencia; la descripción de los datos debe ser detallada, también se debe especificar el sistema de tratamiento, los servicios o unidades ante los que se pueden ejercer los derechos de acceso, rectificación, cancelación y oposición y además se indicará el nivel de las medidas de seguridad (arts. 20.2 LOPD y 54 RLOPD).

Pese a que en el contenido de la disposición general se precisa que debe indicarse "la identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos" (art. 54.1.a RLOPD), ni en el artículo 20 LOPD ni en las disposiciones relativas al contenido de la notificación de ficheros de titularidad privada se hace alusión al tratamiento. Como ya se ha indicado anteriormente, cuando no exista fichero, sino únicamente tratamiento, el responsable del tratamiento no deberá cumplir con esta obligación de notificación[937].

Respecto a los ficheros de titularidad privada, el contenido de la notificación es básicamente el mismo que para los ficheros de titularidad pública (art. 26.2 LOPD y 55.2 RLOPD). No obstante, se añade la identificación del encargado del tratamiento donde se encuentre ubicado el fichero.

2.4.2. Publicidad de la información de los tratamientos

La publicidad de la información de los tratamientos se garantiza en la legislación española mediante el Registro General de Protección de Datos, órgano integrado en la AEPD que tiene como finalidad la inscripción de, entre otros aspectos, los ficheros de titularidad pública y privada[938]. También las leyes autonómicas han creado sus correspondientes registros en los que se inscriben los ficheros de sus ámbitos

[937] Ver Capítulo III.

[938] Así lo dispone el artículo 39.2 LOPD que además también considera objeto de inscripción las autorizaciones que se establezcan en la LOPD, los códigos tipo y los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

competenciales y se ha establecido una cooperación entre las autoridades para mantener actualizadas sus inscripciones[939].

La naturaleza de la inscripción en el registro es declarativa, no constitutiva, de forma que para que sea válido un fichero no es preciso notificarlo[940]. No obstante, se establece la posibilidad de denegar la inscripción si de los documentos que aporta el responsable del fichero se desprende que la notificación no resulta acorde con la LOPD (art. 133 RLOPD), por lo que la AEPD podrá comprobar si hay algún incumplimiento manifiesto y rechazar la notificación[941]. La consecuencia de no cumplir con esta obligación de notificación será el incumplimiento de una obligación legal que conllevará una sanción estipulada en la LOPD[942]. En este sentido, la inscripción en el Registro General de Protección de Datos no exime al responsable del cumplimiento del resto de las obligaciones previstas en la LOPD (art. 60.3 RLOPD).

3. OBLIGACIONES DE CARÁCTER TRANSVERSAL RESPECTO AL CICLO DEL TRATAMIENTO

3.1. El respeto a los principios relativos a la calidad de los datos[943]

3.1.1. Principios de lealtad y licitud

Los principios de lealtad y licitud se establecen de manera negativa. Es decir, lo que se hace es prohibir la recogida de datos por medios fraudulentos, desleales o ilícitos (art. 4.7 LOPD), en vez de establecer la obligación de tratar los datos de manera leal y

[939] El Registre de Protecció de Dades de Catalunya (art. 11 Ley catalana) y el Registro de Protección de Datos (art. 18 Ley vasca).
[940] J. APARICIO SALOM, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, 4ª ed., *op. cit.*, pág. 194.
[941] En la práctica la AEPD revisa si hay incoherencias o si hay contradicciones en la notificación y suele pedir aclaraciones o subsanaciones.
[942] Se considera infracción leve no solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos (art. 44.2.b LOPD) lo que puede ser sancionado con multa de 900 a 40.000 euros (art. 45.1 LOPD).
[943] Se han incluido las obligaciones respecto al principio de calidad en este apartado de obligaciones transversales, aunque, como se verá, en algunas previsiones de la legislación se realiza un enfoque más orientado a alguna determinada fase del ciclo lógico, como puede ser la fase de recogida de los datos. No obstante, con el fin de no fraccionar la exposición se ha estimado conveniente incluir la regulación completa, de forma que pesa más la transversalidad, que la especialidad.

lícita (art. 6.1.a Directiva 95/46/CE). No obstante, se recoge, tanto en este sentido positivo, como en el negativo, en el artículo 8.1 RLOPD.

Así se corrige el hecho de que la prohibición que establece el artículo 4.7 LOPD se refiere a la "recogida" de datos, por lo que se focaliza esta prohibición en esta operación, no en el resto del tratamiento. La Directiva 95/46/CE se refiere al tratamiento en general. Por ello, el artículo 8.1 RLOPD recogió el precepto, tal cual se establece en la Directiva 95/46/CE y añadió lo que se encontraba en el artículo 4.7 LOPD.

Otra diferencia respecto a la Directiva 95/46/CE es que la LOPD, además de referirse a la recogida de datos, lo que prohíbe es la utilización de "medios" fraudulentos, desleales o ilícitos, no se refiere al tratamiento fraudulento, desleal o ilícito[944]. De esta forma, se describen tres comportamientos distintos. El uso de medios fraudulentos supone que se consiguen obtener los datos mediante engaño o fraude. Así se confirma mediante la tipificación en la LOPD de esta conducta como una infracción sancionable como muy grave[945]. La deslealtad significa la falta de observancia de la confianza que alguien debe a otra persona y el término ilícito se define como no permitido legal o moralmente[946]. Sin embargo ni la ilicitud ni la deslealtad se incluyen en la tipificación mencionada en la LOPD.

3.1.2. Principio de finalidad

La LOPD une dos principios que, en la Directiva 95/46/CE, se encuentran en apartados separados (apartados b y c del art. 6.1 Directiva 95/46/CE), los principios de calidad *strictu sensu* y finalidad: "los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados,

[944] J. APARICIO SALOM, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, 4ª ed., *op. cit.*, págs. 238 a 239.
[945] Asi el artículo 44.4.a) LOPD establece como una infracción muy grave "la recogida de datos en forma engañosa o fraudulenta", sancionable con multa de 300.001 a 600.000 euros. De esta forma lo que se sanciona es la recogida de datos y no el uso de medios fraudulentos, que prohíbe el artículo 4.7 LOPD. La Audiencia Nacional, en un asunto en el que no se había podido acreditar cómo una empresa había obtenido los datos del afectado, afirmó que esto no era suficiente para calificar esta conducta como una recogida de datos fraudulenta que exigía de un plus, un especial elemento agravante o cualificado que lo diferencie de una infracción por un tratamiento sin consentimiento que se tipifica como infracción grave. SAN de 23 de septiembre de 2008 (Sala de lo contencioso-administrativo) (ROJ: SAN 3728/2008), FJ 4.
[946] J. APARICIO SALOM, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, 4ª ed., *op. cit.*, págs. 239 a 240.

pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido" (art. 4.1 LOPD).

De nuevo el RLOPD corrige el defecto, ya que, al ligar esos dos principios, los adjetivos de las finalidades servían únicamente para examinar si los datos eran adecuados, pertinentes y no excesivos. Por eso, el artículo 8.2 RLOPD incluye únicamente el principio de finalidad y establece que "los datos de carácter personal sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento".

Para la comprensión de los adjetivos "determinadas, explícitas y legítimas" hay que tener en cuenta que se proyectan en la recogida de datos. De esta forma, se deduce que estos requisitos se deben cumplir frente al interesado de quien se recaban datos, de forma, que el hecho de que las finalidades sean "determinadas" implica que quede claro frente al interesado de qué finalidades se trata exactamente. Lo mismo se puede indicar respecto al adjetivo "explícitas", que supone que estas finalidades deben expresarse de forma clara y expresa. Más problemática conlleva interpretar el adjetivo legítimas, que podría entenderse como el respeto de otras legislaciones, como indicaba el GA29, respecto a la Directiva 95/46/CE[947].

La LOPD establece que los datos "no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos" (art. 4.2

[947] Ver Capítulo V. APARICIO SALOM entiende que finalidades determinadas, explícitas y legítimas significa finalidades declaradas en la inscripción o creación del fichero (determinadas), informadas abiertamente al interesado (explícitas) y adecuadas al ordenamiento jurídico (legítimas). *Ibídem*, pág. 224. TRONCOSO REIGADA considera que una finalidad, para que sea legítima, debe estar ajustada a la Constitución y a la ley. Respecto a los ficheros privados es complejo determinar qué se entiende por finalidad legítima: lo que entre dentro del objeto social de la entidad, en virtud de la libertad de empresa. En los ficheros públicos, para que una finalidad sea legítima, es necesario que responda a una competencia del órgano administrativo (que enlaza con el principio alemán de reserva de administración o *verwaltungsvorbehalt*). Así, la Administración no tiene competencia, por ejemplo, para desarrollar una actividad de marketing político con el registro de población o con el padrón municipal. En el ámbito público, en ocasiones, la ley, no sólo establece la finalidad del fichero, sino que también obliga a llevar a cabo determinados tratamientos de datos. Estos dejan de ser una opción legítima, para convertirse en una exigencia legal a la que el ciudadano tiene derecho, cita como ejemplo la finalidad de la historia clínica definida en la Ley 41/2002, de 14 de noviembre, básica reguladra de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (BOE núm. 274 de 15.11.2002) o la finalidad del Padrón Municipal, recogida en los artículos 15 y 16 de la Ley 7/1985, de 2 de abril, reguladora de las bases de régimen local (BOE núm. 80 de 3.4.1985). A. TRONCOSO REIGADA, "El principio de calidad de los datos", en A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, *op. cit.*, pág. 343.

LOPD), regla que se reproduce en el artículo 8.3 RLOPD. De acuerdo con lo que se indicaba respecto a la interpretación del artículo 6.1.b Directiva 95/46/CE esto impedía tratamientos ulteriores de datos posteriores a la recogida, cuya finalidad fuera incompatible con la originaria. Sin embargo, el TC que consideró este principio parte del contenido esencial del derecho de protección de datos, aludió al término "distinto", por lo que así se ha interpretado, pese a que no se ajustaría al significado de incompatibilidad de la Directiva 95/46/CE que es más amplia[948].

A esta divergencia interpretativa se añade otra de gran calado. El GA29 ha interpretado que los principios de legitimación y calidad de datos, establecidos en los artículos 6 y 7 Directiva 95/46/CE, son de carácter acumulativo[949]. Ello tiene importantes consecuencias para la limitación de los fines de tratamientos ulteriores, ya que supone que además de valorar si el fin del tratamiento ulterior es compatible con el inicial, debe asegurarse que este fin cuenta con una base jurídica válida. Además, en caso de que se considere que el fin del tratamiento ulterior es incompatible con el fin del tratamiento inicial, no podrá salvarse este tratamiento únicamente con la acogida de una base jurídica válida de las establecidas en el artículo 7 Directiva 95/46/CE. Por tanto, simplemente, no podría llevarse a cabo ese tratamiento[950]. Pues bien, la interpretación que sigue la AEPD y los tribunales es que si el fin del tratamiento ulterior es incompatible, es decir, distinto, del fin del tratamiento inicial, cabe acudir a una nueva base jurídica que legitime este tratamiento ulterior[951].

[948] Esta es la interpretación que sigue la AEPD, en virtud de la STC 292/2000, de 30 de noviembre de 2000, que indica que "La llamada libertad informática es así derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención"[948]. Asimismo, este sentencia también indica que "la cesión de los mismos (datos) a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recogida, aun cuando puedan ser compatibles con éstos (art. 4.2 LOPD), supone una nueva posesión y uso que requiere el consentimiento del interesado". Si bien ya en las sentencias referidas al caso RENFE se afirmó este principio, cuando se estableció que los datos relativos a las filiaciones sindicales no podían ser utilizados para finalidades distintas de las que legítimamente justificaron su obtención. Estos datos se utilizaron para detraer de los salarios el importe relativo a la duración de la huelga que afectó a trabajadores que no tomaron parte en ella. STC 11/1998, de 13 de enero de 1998, FJ 7.

[949] Ver CAP V.

[950] *Ibídem.*

[951] SAN de 11 de febrero de 2004 (Sala de lo contencioso-administrativo) (ROJ: SAN 845/2004), FJ 4, que se refiere a la posibilidad de recoger el consentimiento para la nueva finalidad y SAN de 17 de marzo de 2004 (Sala de lo contencioso-administrativo) (ROJ: SAN 1914/2004), FFJJ 3, 4, que especifica que el término incompatibles debe interpretarse como distintas, citadas en la Resolución de la AEPD R/02892/2013 de 18 de diciembre de 2013, en Procedimiento nº PS/00345/2013, FJ XII.

Como en la Directiva 95/46/CE, se establece en la LOPD la excepción relativa a los tratamientos de datos con fines estadísticos, históricos o científicos que no se considerarán incompatibles (art. 4.2 LOPD). No obstante, la determinación de cuando se estará ante estos fines no se deja en manos del responsable, sino que se estará a la legislación sectorial.

3.1.3. Principio de calidad stricto sensu

Los datos de carácter personal que se recojan y se traten deben ser adecuados, pertinentes y no excesivos respecto al ámbito y a las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido y además serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado (art. 4. 1 y .3 LOPD). Si los datos son inexactos o incompletos deberán ser cancelados y sustituidos de oficio por los datos rectificados o completados.

El RLOPD desarrolla el precepto y establece un plazo para que de oficio se proceda a esta corrección, que será de diez días desde que se tuviese conocimiento de la inexactitud, a no ser que la legislación aplicable al fichero estableciera otro plazo (art. 8.5 RLOPD). En caso de que el responsable hubiera comunicado estos datos, deberá poner en conocimiento del cesionario, en un plazo de diez días, esta rectificación o cancelación y este cesionario tendrá a su vez diez días para proceder a la rectificación o cancelación notificada. Por tanto, lo que se hace es equiparar esta obligación de rectificar o cancelar los datos de oficio con el ejercicio de derechos por parte del interesado. No obstante, debido a que se trata de una obligación que se realiza de oficio se indica que no debe comunicarse esta operación al interesado.

Se considerarán exactos los datos que proporcione el afectado. De esta forma, se protege al responsable de la situación en la que el interesado aporte datos falsos o inexactos que pudieran hacer que incurriera en un incumplimiento de esta obligación de calidad.

Respecto a los ficheros de solvencia, en la regulación especial de la LOPD, hay que mencionar el reforzamiento del principio de calidad, debido a que es esencial en este ámbito que los datos sean correctos. Sólo podrán tratarse aquellos datos que respondan

con veracidad a la situación de la deuda en cada momento concreto (arts. 29.4 LOPD y 41 RLOPD). La inexactitud de los datos relativos a una deuda puede conllevar la inclusión incorrecta en un fichero común, que ocasione una vulneración del derecho al honor a través del derecho de protección de datos, en su vertiente instrumental[952].

En los casos en que los servicios de información de solvencia se proporcionan gracias a que son los acreedores los que entregan los datos sobre los deudores, es a éstos a quienes se obliga a cumplir con esta obligación (art. 43.2 RLOPD). Hay que considerar que estos acreedores son responsables del tratamiento, pese a que no se les denomine así en la regulación[953].

3.1.4. Principio de conservación limitada

El principio de calidad también especifica que:

> "los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados" (art. 4.5 LOPD).

El responsable deberá determinar cuando deja de ser necesario el tratamiento de los datos para la finalidad proyectada en el momento de recogida de los datos. También debe tener en cuenta el contexto legal y contractual en el que se enmarca esa finalidad, para fijar el plazo en el que deberá conservar esos datos (arts. 16.5 LOPD y 8.6 RLOPD)[954]. Sin embargo, la cancelación, una vez desaparezca esta finalidad, no

[952] Ver Capítulo VII.
[953] Ver Capítulo III.
[954] De nuevo hay que mencionar los ficheros de solvencia, en los que se encuentra un ejemplo de determinación de plazo de conservación. En este ámbito deben cancelarse los datos referidos a la deuda cuando se produzca su pago o cumplimiento o cuando hubieran transcurrido seis años desde el vencimiento de la obligación o del plazo concreto si fuera de vencimiento periódico (arts. 29.4 LOPD y 41 RLOPD). En los ficheros de las Fuerzas y Cuerpos de Seguridad se obliga a cancelar los datos personales con fines policiales cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento (art. 22.4 LOPD). Para determinar este momento se indican algunos criterios que pueden ser tenidos en cuenta: la edad del afectado, el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de la investigación o procedimiento concreto, la resolución judicial firme (en especial la absolutoria), el indulto, la rehabilitación y la prescripción de responsabilidad. Por último, en los ficheros de publicidad se posibilita que los responsables a quienes el interesado haya manifestado su negativa a recibir publicidad puedan conservar los datos imprescindibles para identificarlo, de forma que eviten volverle a enviarle comunicaciones (art. 48 RLOPD).

implicará la automática supresión de los datos de forma definitiva, sino que se ha establecido la obligación de bloqueo.

El bloqueo es una operación de tratamiento, que consiste en la retención de los datos que no podrán ser tratados excepto para ponerlos a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades que nazcan del tratamiento, durante el plazo de prescripción de estas responsabilidades (arts. 16.3 LOPD y 5.1.b) RLOPD)[955]. Transcurrido este plazo deberán suprimirse los datos.

Mientras no se proceda a la cancelación de los datos, estos deben tratarse de forma que permitan el ejercicio del derecho de acceso (art. 4.6 LOPD y 8.7 RLOPD). Por lo tanto, los datos que se retengan deben ser mantenidos, de forma que puedan ser manipulados para posibilitar este ejercicio, si lo solicita algún afectado.

El responsable tiene también la posibilidad de mantener más tiempo los datos si así lo solicita a la autoridad de control competente, en virtud de su valor histórico, estadístico o científico, de acuerdo con las leyes que regulan la función estadística pública, el patrimonio histórico español y el fomento de la investigación científica y técnica (arts. 4.5 LOPD y 9 RLOPD)[956].

3.2. Atención de los derechos del interesado

3.2.1. Los derechos de acceso, rectificación, cancelación y oposición o derechos ARCO

Los derechos de acceso, rectificación, cancelación y oposición o derechos ARCO, como los denomina la doctrina, han sido considerados parte del contenido esencial del derecho de protección de datos[957]. Constituyen el haz de facultades que se otorga a los titulares de datos para ejercer su poder de disposición sobre los datos personales.

[955] Si bien el artículo 8.6 RLOPD remite a la obligación de bloqueo prevista en la LOPD y el RLOPD, lo cierto es que en el RLOPD la obligación se encuentra en una de las definiciones, lo que parece muy adecuado.
[956] El procedimiento que debe seguir el responsable se establece en los artículos 157 y 158 RLOPD.
[957] STC 254/1993, de 20 de julio de 1993, FJ 7 y STC 292/2000, de 30 de noviembre de 2000, FFJJ 6,7.

Si en la Directiva 95/46/CE, en el derecho de acceso se incluía la capacidad del interesado de solicitar la rectificación, supresión o el bloqueo de los datos (art. 12.b) Directiva 95/46/CE), en la legislación española se establece una regulación autónoma para estas facultades, que se configuran como derechos totalmente independientes[958].

Estos derechos sólo pueden ser ejercidos por los titulares de los datos, ya que se consideran derechos personalísimos. Por ello, es preciso que quien ejerza el derecho acredite su identidad (art. 23.2.a RLOPD), si bien se desarrolla toda una regulación sobre las posibilidades de representación legal y voluntaria (art. 23.2 RLOPD). Si el afectado no acreditase su identidad o no se pudiera verificar la representación, la consecuencia será la denegación del derecho (art. 23.3 RLOPD).

El ejercicio de estos derechos ARCO deberá realizarse a través de medios sencillos y gratuitos que el responsable deberá poner a disposición del afectado (art. 24.2 RLOPD)[959]. La solicitud que debe dirigir el interesado al responsable deberá incluir un contenido mínimo (art. 25.1 RLOPD)[960], aunque en caso de no respetarlo, el responsable

[958] Esta configuración como derechos independientes la deja clara el artículo 24.1 RLOPD que explica que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

[959] Después de indicar que el medio para ejercer el derecho debe ser gratuito se especifica que no puede suponer un ingreso adicional para el responsable el tratamiento (art. 24.3 RLOPD). Y es que aunque no puedan suponer un ingreso para el responsable, la utilización de los medios normalmente llevará algún tipo de coste para el interesado (el sello de una carta normal o el coste de una llamada). Lo que requiere es que no se grave al interesado de forma innecesaria. Se rechazan, por tanto, medios como el envío de cartas certificadas, la utilización de servicios de telecomunicaciones que implique una tarificación adicional o cualesquiera otros medios que impliquen un coste excesivo. La alusión a estos medios en concreto es fruto de la experiencia de la AEPD y que se plasmó en la elaboración del RLOPD, ya que los responsables recurrían a este tipo de medios habitualmente. Otro aspecto que se plasmó en esta regulación del RLOPD es el supuesto en el que un responsable que dispone de un servicio de atención al cliente deniega al interesado la posibilidad de que ejercite los derechos a través de este servicio y planteando, por tanto, una vía diferente. De acuerdo con el artículo 24.4 RLOPD extiende, por tanto, la posibilidad de utilizar estos servicios por parte de los interesados para ejercitar sus derechos, así como los procedimientos de ejercicio de reclamaciones, aunque sólo se contempla como una opción que puede elegir el responsable. Ahora bien, se obliga al responsable a atender la solicitud del interesado aunque no hubiera utilizado el procedimiento establecido para ello por el responsable con los únicos requisitos de que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud y siempre que incluya el contenido preceptivo la solicitud (art. 24.5 RLOPD). Si bien esta obligación del responsable contribuye a garantizar el ejercicio de los derechos, obliga al interesado, esta vez, a incurrir en un coste cuando ejercite el derecho, ya que lo normal es que para acreditar el envío y la recepción deba contratar un servicio más gravoso que un envío normal.

[960] Este contenido será el siguiente: "a) Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente. El párrafo anterior se entenderá sin perjuicio de la normativa específica aplicable a la comprobación de datos de identidad por las Administraciones Públicas en los procedimientos administrativos. b) Petición en que se concreta la

deberá otorgar al interesado la posibilidad de subsanar los defectos de la misma (art. 25.3 RLOPD). La carga de la prueba de que ha respondido, corresponderá al responsable del tratamiento (art. 25.5 RLOPD)

También se dispone que si los interesados ejercieran alguno de estos derechos ante un encargado del tratamiento, este encargado estará obligado a trasladar la solicitud al responsable para que resuelva (art. 26 RLOPD). No obstante, se deja la posibilidad de que el responsable pudiera disponer que el encargado del tratamiento se hiciera cargo de la atención de estas solicitudes.

En la regulación especial de los ficheros de titularidad privada, encontramos excepciones al ejercicio de los derechos ARCO respecto a los ficheros policiales y los de la Hacienda Pública. Los responsables de ficheros policiales podrán denegar el acceso, rectificación y cancelación, respecto a datos tratados con fines policiales, en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones (art. 23.2 LOPD)[961].

Los responsables de ficheros de la Hacienda Pública podrán también denegar el ejercicio de los derechos mencionados cuando obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y cuando el afectado esté siendo objeto de actuaciones inspectoras (art. 23.2 LOPD).

Respecto a las disposiciones sectoriales relativas al sector de información sobre solvencia patrimonial y crédito y al de la publicidad, también encontramos especialidades entorno a los derechos ARCO. Estas previsiones se adaptan a los casos de corresponsabilidad en estos ámbitos, de forma que identifican los papeles que en materia de ejercicio de derechos ostentarán las diferentes entidades implicadas.

---

solicitud.c) Dirección a efectos de notificaciones, fecha y firma del solicitante. d) Documentos acreditativos de la petición que formula, en su caso."

[961] Ha criticado la amplitud de esta excepción que también se refiere a datos especialmente protegidos M.M. SERRANO PÉREZ, *El derecho fundamental a la protección de datos. Derecho español y comparado*, *op. cit.*, págs. 404 a 409.

Así, en el sector de solvencia, se indica el alcance de los derechos que deben atender, tanto quien proporciona los datos al prestador del servicio, como éste mismo. Se tiene en cuenta que el prestador es quien detenta el fichero y, por lo tanto, quien tendrá la posibilidad de proporcionar la información más completa al afectado (arts. 29.3 LOPD y 37.2, 44 RLOPD). En el sector de la publicidad, de igual manera, se tiene en cuenta quién es el que detenta el fichero para vehicular hacia él las solicitudes de ejercicio de derechos (art. 50 RLOPD). En este sector adquiere gran relevancia el derecho de oposición como se comentará más adelante.

a. El derecho de acceso

El derecho de acceso es el que tiene el interesado a solicitar y obtener información sobre si sus propios datos son objeto de tratamiento, la finalidad de este tratamiento, la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos[962], así como sobre los datos objeto del tratamiento[963]. Se deja claro que este derecho es independiente del conocido derecho de acceso administrativo, por lo que para ejercitar ese derecho deberá atenderse a su regulación específica (art. 27.3 RLOPD). No obstante, hay que resaltar la indudable conexión entre ambos derechos, de forma que la protección de datos limitará el otorgamiento del derecho de acceso administrativo[964].

[962] ARENAS RAMIRO indica que, pese a que la referencia a "las comunicaciones realizadas o previstas" parece que, por lógica, debería referirse a las cesiones y no a los accesos por cuenta de terceros que sufran los datos, es decir, los realizados por encargados del tratamiento, menciona la postura contraria de los tribunales. No obstante, esta autora señala que los tribunales mantienen una postura contraria. M. ARENAS RAMIRO, "El derecho de acceso", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, pág. 1167 y SAN de 9 de junio de 2004 (Sala de lo contencioso-administrativo) (ROJ: SAN 4112/2004), FJ 5. Sin embargo, entiendo que hay que tener en cuenta el artículo 29.3 RLOPD que especifica que la información que debe proporcionarse comprenderá "la información disponible sobre el origen de los datos, los cesionarios de los mismos", lo que dejaría claramente fuera a los encargados del tratamiento. Sin embargo, como ya he indicado anteriormente, la Directiva 95/46/CE exigiría informar sobre los encargados del tratamiento e incluso sobre los empleados que acceden a los datos porque así lo establece el concepto de destinatario que no está ligado a las cesiones de datos, sólo se ha creado para dar más transparencia al interesado. Este aspecto no se ha acogido en la legislación española, en la que el concepto de destinatario (o cesionario) se ha ligado a la comunicación de datos.

[963] El interesado podrá solicitar información sobre datos concretos, datos incluidos en un fichero en general o todos los datos que pueda tratar el responsable. No obstante, se establece que el responsable por razones de especial complejidad podrá solicitar al interesado que especifique los ficheros respecto de los que quiere ejercitar el derecho (art. 27.2 RLOPD). Además se establece que deben proporcionarse todos los datos de base del interesado y también los resultantes de cualquier elaboración o proceso informático (art. 29.3 RLOPD).

[964] La Ley 29/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (BOE núm. 295 de 10.12.2013) incluye un precepto (artículo 15) dedicado a la protección de datos

El responsable debe responder al interesado, en un plazo de un mes desde que recibe la solicitud, incluso aunque no dispusiera de datos (art. 29.1 RLOPD). En caso de que la solicitud fuera estimada, el responsable tendrá diez días para hacer efectivo el acceso (art. 29.2 RLOPD). La información se debe proporcionar de forma legible y el interesado puede solicitar la forma en la que quiere recibirla, aunque se deja la puerta abierta a que se puedan restringir los sistemas de consulta, en función de la configuración del fichero[965].

Las causas de denegación son las siguientes: cuando el derecho se haya ejercido en los doce meses anteriores, salvo que se acredite un interés legítimo, cuando lo prevea una ley o una norma de derecho comunitario de aplicación directa, o cuando estas normas impidieran al responsable revelar los datos (art. 30 RLOPD).

b. Los derechos de rectificación y cancelación

Los derechos de rectificación y cancelación tienen una regulación común, ya que están conectados. El derecho de rectificación comporta el derecho por parte del interesado de que se modifiquen sus datos, si estos resultaran inexactos o incompletos. El derecho de cancelación comporta la supresión o el bloqueo de los datos que resulten inadecuados o excesivos (arts. 16 LOPD y 31 RLOPD). Ambos derechos, por tanto, están relacionados con los principios de calidad.

El interesado, en su solicitud, deberá identificar claramente los datos que pretende que se rectifiquen o se cancelen, así como aportar documentación que justifique esta

personales, con el fin de establecer criterios para realizar la ponderación. Además el Consejo de Transparencia y Buen Gobierno, incorpora a un representante de la AEPD y se ha establecido entre este órgano y la AEPD una colaboración para adoptar los criterios de aplicación del precepto mencionado, en particular en lo que respecta a la ponderación entre el interés público en el acceso a la información y la garantía de los derechos de los interesados (Disposición Adicional 5ª Ley 29/2013). De igual forma, la Ley 19/2014, del 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno (DOGC núm. 6780 de 31.12.2014) también incorpora en sus artículos 23 y 24 criterios para realizar la ponderación mencionada. Las resoluciones sobre el derecho de acceso pueden ser objeto de reclamación ante la Comissió de Garantia del Dret d'Accés a la Informació Pública, órgano creado a estos efectos (art. 39 Ley 19/2014). En caso de que la denegación que hubiera producido la reclamación se hubiera debido a la protección de datos, la Comissió tendrá que pedir informe a la ACPD (art. 42.8 Ley 19/2014).

[965] Las opciones que puede elegir el interesado están desglosadas en el artículo 28.1 RLOPD: visualización en pantalla; escrito, copia o fotocopia remitida por correo, certificado o no; telecopia; correo electrónico y otros sistemas de comunicación electrónicas; cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.

solicitud. El responsable dará respuesta a esta solicitud en el plazo de diez días, de nuevo, incluso aunque no contara con datos del interesado. El responsable podrá denegar el derecho de cancelación cuando los datos deban ser conservados, de acuerdo con las disposiciones legales aplicables o, en virtud, de las relaciones contractuales entre el responsable y el interesado que justificaron el tratamiento (art. 33.1 RLOPD), cuando así lo prevea una ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan revelar a los afectados el tratamiento de los datos a los que se refiera el acceso (art. 33.2 RLOPD)[966].

Si se otorga la cancelación, el responsable, de todas formas, no debe proceder a la supresión, sino al bloqueo de los datos, ya que debe conservar los datos a disposición de las administraciones públicas, jueces y tribunales, para dirimir posibles responsabilidades que nazcan del tratamiento (art. 16.3 LOPD). Esta disposición limita el plazo de bloqueo al plazo de prescripción de las responsabilidades y, una vez cumplido este plazo, entonces el responsable procederá a la supresión de los datos.

Se establece, al igual que en el artículo 12.b Directiva 95/46/CE, que en caso de que el responsable hubiera cedido previamente los datos, deberá comunicar la rectificación o cancelación al cesionario, en un plazo de diez días para que éste, en un nuevo plazo de diez días, proceda a realizar la misma operación (art. 32.3 RLOPD). No se exige, sin embargo, que el cesionario comunique al interesado que ha llevado a cabo esta operación.

Por último, indicar que, debido a lo granado de este catálogo de derechos, en ocasiones el interesado no interpondrá correctamente las solicitudes de ejercicio de derecho y el responsable se verá ante el dilema de aceptar la solicitud o denegarla por una incorrecta interposición. Esta situación se refleja también en la regulación, de forma que, respecto a este derecho de cancelación, se especifica que, en caso de que el interesado ejerciera este derecho, pero con la finalidad de revocar el consentimiento, deberá seguirse la regulación de la LOPD y el RLOPD (art. 31 RLOPD).

[966] Esta última causa de denegación parece tratarse de un error del legislador que hubiera copiado en este apartado lo mismo que se indicó en sede de la regulación del derecho de acceso, al que se hace referencia, ya que no tendría mucho sentido esta redacción. Más bien parece que lo que debería indicar es que el responsable pudiera denegar el ejercicio del derecho cuando estas normativas impidan al responsable realizar las operaciones que el interesado le demanda o cuando estas normativas le impidieran al responsable revelar siquiera que trata datos del interesado.

c. El derecho de oposición y el derecho de impugnación de valoraciones

El derecho de oposición se contempla como un derecho de cancelación referido, no obstante, a aquellos supuestos de legitimación del tratamiento de datos que no consistan en el otorgamiento del consentimiento del interesado (art. 6.4 LOPD). Por tanto, se trata de un derecho que pretende suplir la falta de intervención del interesado, de forma que, incluso en aquellos supuestos que permitan el tratamiento de datos por vías diversas al consentimiento, se otorgue al interesado la posibilidad de negarse. Sin embargo, no es un derecho que pueda ejercerse en cualquier caso, sino que contará con unas limitaciones. De esta forma, se exige que el interesado cuente con motivos fundados y legítimos relativos a una concreta situación personal.

Adicionalmente a esta regulación, se establece también el derecho de oposición en el ámbito de los tratamientos de datos con fines de publicidad y de prospección comercial que, en la Directiva 95/46/CE, se incluía en el mismo artículo 14 que regulaba el derecho de oposición. Los interesados tienen derecho a oponerse a este tipo de tratamientos, lo que implica, la cancelación de los datos de forma automática (art. 30.4 LOPD). Es decir, en este caso, no se precisará ningún motivo que justifique la solicitud.

Hay que tener en cuenta que esta disposición se incluye entre las previsiones relativas a ficheros de titularidad privada, por lo que sólo sería aplicable a este tipo de ficheros. Es cierto que estos fines parecen propios de responsables de este sector pero también las administraciones públicas realizan estas actividades y no parece acertado extraerlas de la posibilidad de ejercer este derecho. En este sentido, el desarrollo previsto del derecho de oposición en el RLOPD no se incorpora en sede de ficheros de titularidad privada (arts. 34 a 36 RLOPD), por lo que no se limita su aplicación a los mismos. De nuevo sería otra licencia que se tomó el legislador al corregir este defecto en la transposición de la Directiva 95/46/CE, pero que pone en entredicho la capacidad de desarrollo reglamentario.

A las dos posibles causas mencionadas, que permiten el ejercicio de este derecho, en la legislación española se añade una tercera: el derecho que la LOPD denomina de

impugnación de valoraciones y que responde al derecho que contempla la Directiva 95/46/CE, en su artículo 15, relativo a las decisiones individuales automatizadas.

El derecho de impugnación de valoraciones es el que tienen los interesados a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de forma significativa, si ésta se adopta, únicamente, en virtud de un tratamiento de datos que persigue evaluar determinados aspectos de su personalidad (art. 13 LOPD)[967]. Hay que resaltar la corrección realizada por el artículo 36 RLOPD que, una vez más ajusta la regulación de la LOPD a lo que establece la Directiva 95/46/CE, de manera que se introduce el adjetivo automatizado -que establece la norma europea y que la LOPD no había incluido- por lo que se podía aplicar a tratamientos automatizados y no automatizados.

Con el mismo objetivo de asimilar la regulación de este derecho a la que se encuentra en el artículo 13.2 Directiva 95/46/CE, el RLOPD establece dos supuestos que permitirán que se someta al interesado a una decisión de este tipo, supuestos que no aparecían en la LOPD. El primero de estos supuestos es si la decisión se adopta en el marco de la celebración o ejecución de un contrato a petición del interesado y si éste puede alegar lo que estime pertinente, a fin de defender su derecho o interés. Además se exige, de forma adicional a lo que establece la Directiva 95/46/CE, que el responsable informe de que se adoptará este tipo de decisiones y que se cancelen los datos en caso de que no llegue a celebrarse el contrato (art. 36.2.a) RLOPD).

El segundo supuesto previsto que permitirá la adopción de este tipo de decisiones es que una norma con rango de ley lo autorice y establezca medidas que garanticen el interés legítimo del interesado, supuesto idéntico al contemplado por la Directiva 95/46/CE (art. 36.2.b) RLOPD).

El derecho de oposición, pese a tener las mismas consecuencias que el derecho de cancelación se diferencia de este, primero, porque como se ha indicado se ejercería para unos determinados supuestos y en función de los motivos expuestos y, segundo, porque lo

[967] El artículo 36 RLOPD, que desarrolla este artículo 13 LOPD, añade algunos ejemplos de lo que se pueden considerar estos aspectos de su personalidad: rendimiento laboral, crédito, fiabilidad o conducta, reproduciendo lo que está en el artículo 15.1 Directiva 95/46/CE.

que pretende inicialmente no es la supresión de los datos, sino el cese del tratamiento de datos. De todas formas, el resultado de la estimación de la solicitud de ejercicio de este derecho supone la exclusión de los datos del interesado del tratamiento realizado por el responsable, lo que necesariamente exigirá su supresión.

d. Tutela

En caso de que se denegara cualquiera de los derechos ARCO[968], o no se respondiera al interesado en los plazos previstos, éste podrá dirigirse a las autoridades de control con el fin de interponer un procedimiento llamado de tutela de los derechos, de forma que será la autoridad de control la que intercederá, en nombre del interesado, para lograr que el responsable le responda o para estimar si la denegación ha sido correcta o, por el contrario, debe ser estimada la solicitud. En este caso, la autoridad de control conminará al responsable a que proceda a la estimación de la solicitud y actúe en consecuencia[969].

Además en la regulación de los diferentes derechos se obliga al responsable a informar al interesado de la posibilidad que tiene de acudir a la AEPD para recabar su tutela si no estuviera de acuerdo con el resultado obtenido.

3.2.2. El derecho de revocación del consentimiento

El artículo 6.3 LOPD contempla la posibilidad de revocar el consentimiento otorgado para permitir el tratamiento de datos personales aunque exige, para ello, causa justificada y no permite la retroactividad de los efectos de esta revocación. Esta escueta regulación se desarrolla en el RLOPD de forma similar a los derechos ARCO. En este sentido, se establece que el ejercicio de este derecho deberá realizarse a través de un

[968] La tutela se ha establecido en la LOPD como un derecho más del Título III pero sólo se refiere a los derechos de oposición, acceso, rectificación o cancelación (art. 18.2 LOPD) aunque, como se ha visto, fruto del desarrollo reglamentario, el derecho de impugnación de valoraciones también se ha vehículado a través del derecho de oposición por lo que se podría interponer también un procedimiento de tutela en virtud de la denegación del derecho de oposición interpuesto con esta causa.
[969] El procedimiento de tutela se regula en los artículos 117 a 119 RLOPD.

medio sencillo, gratuito y que no implique ningún ingreso al responsable (art. 17.1 RLOPD)[970].

El responsable tendrá un plazo de diez días para cesar en el tratamiento de los datos, aunque deberá tener en cuenta la obligación de bloqueo de los datos, conforme al artículo 16.3 LOPD (art. 17.2 RLOPD). Como rasgo específico de este derecho se establece que si el interesado solicitara confirmación del cese en el tratamiento, el responsable deberá responder esta solicitud (art. 17.3 RLOPD). Por último, si los datos se hubieran cedido el responsable deberá comunicar al cesionario en diez días la revocación para que éste en otros diez días también cese en el tratamiento (art. 17.4 RLOPD).

3.3. El deber de confidencialidad y de seguridad del tratamiento

3.3.1. El deber de confidencialidad

En la legislación española la obligación de confidencialidad se configura como el deber de secreto profesional que deben respetar el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de datos (art. 10 LOPD)[971]. Por tanto, el contenido de la misma difiere totalmente del que tiene en la Directiva 95/46/CE, que la configura como una obligación de subordinación.

Además del responsable, hay otros sujetos obligados que son "quienes intervengan el cualquier fase del tratamiento", entre quienes debe incluirse el encargado del tratamiento. No obstante, aunque se establezca esta obligación para otras personas distintas al responsable y al encargado, no se corresponde, en estos casos, con ninguna responsabilidad administrativa en materia de protección de datos.

[970] Se enumeran ejemplos de los medios que se consideran aceptables: un envío prefranqueado, una llamada a un número de teléfono gratuito o a los servicios de atención al público que hubiera establecido. Se repiten además los medios no considerados aceptables que se especifican en el artículo 24.3 RLOPD ya referido.

[971] La Audiencia Nacional relaciona este deber de secreto del artículo 10 LOPD con el secreto profesional que según indica el ATC de 11 de diciembre de 1989 "se entiende como la sustracción al conocimiento ajeno, justificada por razón de una actividad, de datos o informaciones obtenidas que conciernen a la vida privada de las personas". SAN de 7 de mayo de 2009 (Sala de lo contencioso-administrativo) (ROJ: SAN 2285/2009), FJ 3.

La obligación de secreto se incumple, tanto si se desvela información a terceros ajenos a la organización del responsable, como a personas de la misma organización que no precisaban del conocimiento de estos datos[972]. No obstante, para considerar que se ha vulnerado el secreto se exige que se acredite que ha existido revelación de los datos a terceros, por lo que se configura como una obligación de resultado[973].

Este deber de secreto profesional se complementa con el deber de guardar los datos que debe entenderse como un deber de custodia. Tanto respecto a esta obligación de custodia como a la de secreto, se indica que subsistirán de forma indefinida, incluso tras la finalización de las relaciones con el titular del fichero o, en su caso, el responsable del mismo. Sin embargo, parece que esta subsistencia sólo tendría sentido respecto al secreto, ya que hay que entender que ya no será preciso respecto a la obligación de custodia.

[972] Como indica el Tribunal Supremo: "la posibilidad de que más individuos de los estrictamente necesarios tengan acceso a datos cubiertos por un deber de secreto constituye una infracción de dicho deber, cualquiera que sea la relación de esos individuos con la organización responsable de los datos." STS de 13 de noviembre de 2012 (Sala 3ª) (ROJ: STS 7404/2012), FJ 2. En este sentido, también cabe mencionar una medida que el RLOPD establece en sede de medidas de seguridad. Así, cuando el responsable tenga personal propio o ajeno que deba realizar tareas que no impliquen el tratamiento de datos debe adoptar las medidas adecuadas para limitar el acceso de este personal a datos, soportes o recursos (art. 83 RLOPD). Cuando este personal sea ajeno, se obliga a que el contrato de prestación de servicios suscrito con el proveedor establezca la prohibición de acceder a datos personales y la obligación de secreto respecto a los datos que ese personal pudiera conocer con motivo de la prestación de servicios. Esta obligación en lo relativo al personal ajeno no repite la necesidad de la adopción de medidas por parte del responsable para evitar el acceso a los datos del mismo, lo que parece que debería cumplirse. Por otro lado, el hecho de establecer una obligación de secreto, implica que habrá un acceso a los datos, que se ha prohibido, lo que tampoco parece lógico.

[973] En este sentido, se han planteado supuestos en los que se ha enviado una carta con datos personales a un domicilio equivocado. El Tribunal Supremo rechazó un recurso de casación interpuesto y confirmó el fallo de la sentencia de la Audiencia Nacional, que consideró que no había habido vulneración del deber de secreto, sino del principio de calidad, al haber remitido, en sobre cerrado, datos personales a un domicilio erróneo. Enviar la información en un sobre cerrado no implicaba, según la Audiencia, ponerla a disposición de la persona que residía en el domicilio, STS de 10 de junio de 2011 (Sala 3ª) (ROJ: STS 3668/2011), FJ 1. También se puede citar una sentencia de la Audiencia Nacional, que considera que el envío en sobre cerrado de datos personales a un domicilio equivocado no supone vulneración del deber de secreto, SAN de 4 de junio de 2008 (Sala de lo contencioso-administrativo) (ROJ: SAN 2243/2008), FJ 4. Por último mencionar otra sentencia de la Audiencia Nacional, que también se refiere al envío de información personal por parte de una entidad bancaria a un cliente y cuyo sobre contaba con una ventanilla transparente, a través de la que quedaron a la vista algunos datos personales. La Audiencia considera que la AEPD no acreditó que se había producido la revelación de datos, ya que el sobre se había entregado ya abierto y además los inspectores indicaron, al inspeccionar los sobres que utilizaba el banco, que no permitían mostrar los datos de la cuenta bancaria. La Audiencia indica que el deber de secreto es una obligación de resultado que exige la revelación de datos. SAN de 7 de mayo de 2009 (Sala de lo contencioso-administrativo) (ROJ: SAN 2285/2009), FJ 3.

Esta última disposición es un tanto confusa, en cuanto reaparece el titular del fichero[974]. Esta figura, que estaba ya en la LORTAD en este mismo precepto, se mantuvo en la LOPD[975]. No se ha dado ninguna relevancia a la misma y la AEPD ha entendido que titular y responsable se refieren al mismo responsable[976].

3.3.2. El deber de seguridad

a. La prevalencia de la regulación frente a la autorregulación

La LOPD enuncia el principio de seguridad de los datos según el que, tanto el responsable del fichero como el encargado del tratamiento, deben adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado (art. 9.1. LOPD). Para ello, debe tenerse en cuenta el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, provengan de la acción humana o del medio físico o natural. Por tanto, esta regulación es muy similar a la de la Directiva 95/46/CE[977].

No obstante, a continuación se prohíbe que se registren datos en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas

[974] Hay que recordar que la LOPD también hacía referencia al titular del fichero en su artículo 25 que establece cuando se pueden crear ficheros de titularidad privada.
[975] Este artículo sólo fue modificado mediante la supresión del término automatizado.
[976] E. DEL PESO NAVARRO, *Ley de Protección de Datos: la nueva LORTAD, op. cit.*, págs. 114 a 115. En este sentido, indicar además que, en el marco de la LORTAD, en los modelos de notificación de ficheros de titularidad privada (no sucedía lo mismo en los modelos para notificar los ficheros de titularidad pública) se leía en las instrucciones, que en el apéndice del formulario se tenían que indicar los datos del "Titular del fichero" y se explicaba que "Se indicará en este apartado la persona física o jurídica responsable del fichero es decir, la que decida sobre su finalidad, contenido y uso. A efectos de esta notificación se entiende que Titular y Responsable son los mismos. El N.I.F./C.I.F. indicado en este apartado debe repetirse en la parte superior de cada hoja del modelo de notificación. Se indicará el C.N.A.E. de acuerdo al R.D. 1.560/1992, de 18 de diciembre." De esta forma en la casilla que figuraba en todas las hojas del formulario para incluir el N.I.F./C.I.F se indicaba "N.I.F./C.I.F. DEL TITULAR" y en el apartado donde se debían incluir los datos del responsable del fichero se especificaba "(A efectos de esta notificación se entiende que Titular y Responsable son los mismos)". Resolución de 22 de junio de 1994, de la Agencia de Protección de Datos, por la que se aprueban los modelos normalizados en soporte papel y magnético a través de los que deben efectuarse las correspondientes inscripciones en el Registro General de Protección de Datos, (BOE de 23.6.1994). También hay que mencionar la Ley vasca que en su artículo 20 se refiere a los titulares de los ficheros, en vez de a los responsables, cuando regula los requerimientos, aunque tampoco parezca que se pueda entender que se trate de otra figura diferenciada.
[977] La única diferencia a destacar es que, en la LOPD, no se incluye como uno de los factores a tener en cuenta el coste que sí se indicaba en el artículo 17.1 Directiva 95/46/CE.

(art. 9.2 LOPD). Por tanto, la obligación se concreta en el cumplimiento de estas condiciones que se han desarrollado en el Título VIII RLOPD. En coherencia con este precepto se ha tipificado la infracción que persigue la vulneración de este principio, que lo que contempla como sancionable es el hecho de no cumplir con las medidas de seguridad que establece el RLOPD[978].

Estas medidas se consideran un conjunto de mínimos y, por tanto, pudiera demandarse del responsable un plus de medidas si fuera necesario, en virtud de los elementos que aportaba el artículo 9.1 LOPD. Esta obligación se ha configurado, por tanto, como una obligación de medios y no como de resultado[979].

La LOPD ha previsto la posibilidad de que los responsables elaboren códigos tipo que pueden incorporar, entre otros aspectos, las "normas de seguridad del entorno, programas o equipos" (art. 32.1 LOPD). Sin embargo, estos códigos van más dirigidos al cumplimiento de los otros principios establecidos en la LOPD. Muestra de ello, es que en el RLOPD se considera como un compromiso adicional que podría incluirse en los códigos, la adopción de medidas de seguridad diferentes a las exigidas legalmente (art. 74 RLOPD).

Al contar con un desarrollo reglamentario con un catálogo exhaustivo de medidas de seguridad, no se ha considerado necesario ahondar en la autorregulación. Se podría decir que, en materia de seguridad, en España se ha optado por la regulación en vez de incentivar la autorregulación. Otro ejemplo de ello es la aprobación, en el ámbito de la administración pública, de leyes que también desarrollan medidas concretas de seguridad[980].

---

[978] Se establece como infracción grave "mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen" (art. 44.3.h LOPD) que se sanciona con multa de 40.001 a 300.000 (art. 45.2 LOPD).

[979] SAN de 7 de mayo de 2009 (Sala de lo contencioso-administrativo) (ROJ: SAN 2285/2009), FJ 3. También lo ha señalado A. TRONCOSO REIGADA, *La protección de datos personales. En busca del equilibrio*, *op. cit.*, pág. 183.

[980] Baste citar el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, (BOE núm. 25 de 29.1.2010, Sec. I Pág. 8089) y el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (BOE núm. 25 de 29.1.2010, Sec. I Pág. 8139).

Esto no significa que no se haya acudido, especialmente en el caso de empresas multinacionales o empresas que se relacionan en un contexto internacional, a la normalización pero ha sido una cuestión ajena a la normativa de protección de datos. En un contexto global, las grandes organizaciones adoptan estos estándares para mantener, en toda su estructura, los mismos niveles de protección de la seguridad de la información[981]. En el entorno de los servicios de *cloud computing,* la AEPD ha indicado que una forma de que el responsable garantice que su proveedor de *cloud computing* cumpla con las medidas de seguridad, es si éste acredita que dispone de una certificación[982]. De ello se deduce que la AEPD acepta que las certificaciones puedan ser válidas para cumplir con lo establecido en el RLOPD[983].

Aparte de la normalización referida a los sistemas de gestión de la seguridad, hay que hacer mención de las certificaciones de personas, que se han desarrollado en el marco de asociaciones privadas. Y es que aunque no se haya adoptado en la legislación española la figura del encargado de protección de datos, que contemplaba la Directiva 95/46/CE, la enorme complejidad de esta normativa y las elevadas sanciones han llevado a muchas empresas y organizaciones a tener que designarlo. En muchos casos se ha asignado este papel a personas de la organización, como una función más, o incluso se ha subcontratado a empresas externas para llevar a cabo esta función. Al no existir ninguna formación

[981] Hay que destacar la certificación UNE-ISO/IEC 27001:2014 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información (SGSI). Requisitos.

[982] Y es que en el sector del *cloud computing* han proliferado especialmente las certificaciones en materia de seguridad. De hecho, una de las líneas de trabajo planteadas por la Comisión Europea para promover en la UE la utilización de estos servicios, de forma que incentivaran la economía, fue "abrirse paso a través de la selva de normas", en referencia a los diferentes estándares existentes. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Liberar el potencial de la computación en nube en Europa, COM(2012) 529 final, Bruselas, 27.9.2012, pág. 11. Fruto de estos trabajos fue la publicación por ENISA de un listado de certificaciones existentes sobre *cloud computing*, que puede consultarse en https://resilience.enisa.europa.eu/cloud-computing-certification.

[983] Aunque no especifica el tipo de certificaciones. Asimismo, en la 4ª Jornada Abierta, celebrada el 27 de abril de 2012, que dedicó la AEPD a los servicios de *cloud computing*, indicó que la adopción de medidas de seguridad por el prestador podía examinarse desde un enfoque funcional y no formal. Guía para clientes que contraten servicios de *Cloud Computing*, Agencia Española de Protección de Datos, 2013, http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf, (fecha consulta: 23.9.2014), pág. 15 y Ponencia de la Jornada Abierta, celebrada el 27 de abril de 2012, sobre *Cloud computing*: Sujetos que intervienen, Ley aplicable, Garantías, J. RUBÍ NAVARRETE, AEPD, pág. 9 http://www.agpd.es/portalwebAGPD/jornadas/4_sesion_abierta_2011/common/CLOUD_COMPUTING.pdf (fecha consulta: 23.9.2014). La ACPD ha indicado que disponer de la certificación ISO/IEC/27011 o de cualquier otra en materia de seguridad no es garantía suficiente de cumplimiento de las medidas de seguridad del RLOPD, por lo que sería preciso realizar una auditoría conforme a la normativa de protección de datos. Dictamen CNS 57/2013 de la ACPD.

específica en esta materia ni tampoco ningún cuerpo oficial de profesionales, se han desarrollado de la mano de organizaciones privadas estas certificaciones[984].

b. Las medidas de seguridad

Las medidas de seguridad se aplican a ficheros automatizados y no automatizados[985] y se agrupan por niveles acumulativos: básico, medio y alto. Lo primero que deberá hacer el responsable, por tanto, es clasificar los ficheros o tratamientos en el nivel adecuado, con el fin de determinar las medidas que deberá adoptar. El más fácil será el nivel básico, ya que todos los ficheros o tratamientos de datos de carácter personal se entenderá que tienen este nivel.

El nivel medio se aplicará a ficheros o tratamientos que podríamos dividir en dos grupos: uno en el que se englobarían aquellos ficheros o tratamientos a los que se aplicaría el nivel medio principalmente por el tipo de datos que se incluyen en los mismos[986] y, otro, en el que se englobarían aquellos fichero o tratamientos que debido al tipo de servicio o actividad del responsable del fichero también exigirían una mayor protección, por el gran volumen de datos o por la especial sensibilidad de los mismos[987] (art. 81.2 RLOPD).

---

[984] Pueden mencionarse las certificaciones de la asociación estadounidense *International Association of Privacy Professionals* (IAPP), entre las que se puede citar la *Certified Information Privacy Professional* (CIPP), en España, la certificación *APEP-Certified Privacy* (ACP) de la Asociación Profesional Española de Privacidad y las certificaciones en materia de seguridad de sistemas de información de la asociación *Information Systems Audit and Control Association* (ISACA), entre las que figura la *Certified Information Systems Auditor* (CISA).

[985] Esta fue una novedad importante que introdujo el RLOPD respecto a su antedecesor, el derogado Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. Pese a que se hable de ficheros (incluso en la infracción tipificada relativa al cumplimiento de medidas de seguridad se habla de mantener los ficheros sin las debidas medidas de seguridad) se especifica en el RLOPD que las medidas serán exigibles a los ficheros y tratamientos (art. 79, 80 RLOPD), lo que es lógico, puesto que no pueden dejarse sin proteger los datos que no consten en ficheros.

[986] De esta forma, en este grupo incluiría los ficheros o tratamientos relativos a la comisión de infracciones administrativas o penales y aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

[987] En este grupo incluiría aquellos ficheros o tratamientos, cuyo funcionamiento se rija por el artículo 29 LOPD, que regula la prestación de servicios de información sobre solvencia patrimonial y crédito; aquéllos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias; aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros y aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

El nivel alto se aplicará a los ficheros o tratamientos de datos especialmente protegidos[988], a los que contengan datos recabados con fines policiales sin consentimiento de las personas afectadas y aquéllos que contengan datos derivados de actos de violencia de género (art. 81.3 RLOPD).

Se aplicará el nivel medio pero, además una medida de nivel alto[989], a los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización[990] (art. 81.4 RLOPD).

Se establece además un régimen específico para algunos ficheros o tratamientos que incluyen datos especialmente protegidos pero a los que, excepcionalmente, se les aplicará el nivel básico. Son aquellos ficheros o tratamientos cuyos datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros y aquellos en los que de forma incidental o accesoria se contengan datos especialmente protegidos sin guardar relación con su finalidad[991] (art. 81.5 RLOPD). También podrá aplicarse sólo nivel básico a aquellos ficheros o tratamientos que contengan datos relativos a la salud, referentes al grado de discapacidad o la simple declaración de discapacidad o invalidez del afectado, con motivo de deberes públicos[992] (art. 81.6 RLOPD).

---

[988] Hay que recordar que estos datos son los de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

[989] En concreto la que se especifica en el artículo 103 RLOPD relativo al registro de accesos.

[990] Además hay que tener en cuenta que estos responsables tendrán que adoptar aquellas medidas de seguridad que establece su propia normativa sectorial. En este sentido el artículo 81.7 RLOPD señala que las medidas que se incluyen en el RLOPD son mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias que resultaran aplicables o las medidas que por propia iniciativa adoptase el proio responsable. En el sector público y, muy especialmente, en toda la normativa relativa a la puesta en marcha de la administración electrónica, habrá que tener en cuenta las normas aprobadas con el objetivo de asegurar la protección de los datos.

[991] Estos supuestos introducidos como novedad en el RLOPD responden a las críticas que las pequeñas empresas y empresarios vertieron sobre el hecho de que el nivel alto, que debería aplicarse en casos excepcionales se aplicaba de forma habitual, ya que cualquiera que tenía que personal a su cargo y tenía que pagar salarios y cumplir con los deberes fiscales debía tratar algún datos especialmente protegido. De esta forma, se pretendía que estos ficheros de nóminas no conllevaran siempre la aplicación del nivel alto. Por eso, se pretende cubrir todas aquellas situaciones que se habían ido planteando en la práctica, como el pago de afiliaciones sindicales por nómina, que se cubriría con este art. 81.5 RLOPD.

[992] En este caso, se perseguía el mismo objetivo mencionado en la nota anterior. Lo que se cubriría sería principalmente la elaboración de declaraciones fiscales, en las que debiera incluirse el dato relativo a la

Una posibilidad que contempla el RLOPD es que, cuando en un sistema de información existan ficheros o tratamientos que, en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente, siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos y que esto se haga constar en el documento de seguridad (art. 81.8 RLOPD)[993].

Una vez el responsable ha analizado el nivel que debe aplicar a los diferentes ficheros o tratamiento deberá acudir a los diversos catálogos establecidos para los niveles. No obstante, el responsable también tendrá que tener en cuenta algunas medidas que no se hayan incluidas en estos niveles, sino que se encuentran en el apartado dedicado a las disposiciones generales. Por ello, hay que entender que son medidas que se aplicarán a todo tipo de fichero o tratamiento, es decir, a efectos prácticos será como si fueran medidas de nivel básico[994].

No me detendré en el detalle de las medidas de seguridad que establece el RLOPD en estos diferentes catálogos, pero sí quiero hacer referencia, de manera general, a las mismas. En primer lugar, se debe asegurar el control de todos los elementos que conforman el sistema de información, por lo que se incluyen obligaciones documentales, de inventario y de llevanza de registros.

---

discapacidad del trabajador o la tramitación de bajas o altas del personal. Sin embargo, se plantearon dudas acerca de los datos concretos que se entendían excepcionados y la AEPD tuvo que emitir informes al respecto para aclarar cual sería su criterio al respecto. La AEPD indicó que estarían incluidos en esta disposición y, por lo tanto, no exigirán aplicar el nivel alto de seguridad los siguientes tipos de datos: aquellos que versen sobre el porcentaje de discapacidad, el hecho de saber si hay discapacidad o no, el dato de apto y no apto, el dato de invalidez, el dato de incapacidad laboral (sólo si o no y la fecha) y el dato de si es enfermedad común, accidente laboral o enfermedad profesional. Contrariamente, cuando se traten datos concretos del accidente de trabajo, como sucede cuando se completa el formulario de notificación del accidente a la mutua o cuando se investiga el accidente, en cumplimiento de la legislación en materia de prevención de riesgos laborales, la AEPD entiende que se deberán adoptar las medidas de nivel alto.

[993] Esta opción es muy interesante para los responsables que, en caso contrario y como sucedía con el anterior reglamento de medidas de seguridad, debían aplicar el nivel a todo el fichero completo, cuando a veces sólo una pequeña parte de los datos era la que revestía estrictamente el nivel mayor de protección.

[994] Estas disposiciones se refieren a los encargados del tratamiento, a las prestaciones de servicios sin acceso a datos personales, a la delegación de autorizaciones, al acceso de datos a través de redes de telecomunicaciones, al régimen de trabajo fuera de los locales del responsable o del encargado del tratamiento y a los ficheros temporales o copias de trabajo de documentos (arts. 82 a 87 RLOPD).

La medida más relevante, en este caso, es el documento de seguridad, que no se incluye en los catálogos por niveles, sino que es de aplicación general. El documento de seguridad es una pieza esencial en la configuración de la protección, ya que es donde se documentarán todas las medidas adoptadas por el responsable para cumplir con la regulación[995]. Será importante incluir todas las políticas y procedimientos que permitan cumplir con las medidas establecidas.

Este documento lo deberán elaborar tanto los responsables, como los encargados del tratamiento y debe incluir un contenido mínimo que se establece en el precepto[996]. Se trata de un documento vivo que debe mantenerse actualizado y que debe ser revisado continuamente[997]. Es necesario que se realice un seguimiento de que se mantiene el nivel de seguridad adecuado, por lo que también se establecen controles periódicos y auditorías. Un registro importante es el de incidencias que también ayudará a detectar los problemas de seguridad que puedan hacer necesario un cambio en las medidas.

Otro grupo de medidas de seguridad serían las lógicas y físicas, como pueden ser la realización de copias de seguridad, los procesos de identificación y autenticación en el acceso a los sistemas, los controles de acceso físico o el cifrado de la información.

[995] De esta forma, se convierte en un instrumento importante a la hora de acreditar este cumplimiento, instrumento que la AEPD demandará al ser obligatoria su llevanza y mediante el que obtendrá las primeras evidencias acerca del cumplimiento por parte del responsable. Y es que, a efectos de responsabilidad, tan importante es el hecho de cumplir las medidas, como el hecho de poder demostrar ese cumplimiento.

[996] El contenido mínimo se especifica en los apartados 3 y 4 del art. 88 RLOPD. Además se establece la posibilidad de que el responsable delegue la llevanza del documento de seguridad en el encargado, si los datos de un fichero o tratamiento se incorporaran, de modo exclusivo, en los sistemas del encargado y ello afectase a parte o a la totalidad de los ficheros o tratamientos del responsable. Este punto debe incluirse en el contrato suscrito entre el responsable y el encargado del tratamiento. Esta redacción es muy confusa ya que no se acierta a entender porque se indica que será posible la delegación si parte o todos los tratamientos o ficheros del responsable están afectados por el hecho de que la totalidad de los datos se incorporen en exclusiva en los sistemas del encargado. Se extrae que el único requisito será este último. Es decir que la totalidad de los datos de un tratamiento o de un fichero se incorporen en exclusiva en los sistemas del encargado. Aumenta la confusión que, a continuación, se especifique que quedarán a salvo los datos contenidos en recursos propios (se entiende recursos del responsable). Es importante tener en cuenta las consecuencias que puede conllevar esta delegación, ya que como indica este precepto, "se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento", lo que implicará la asunción de la responsabilidad por parte del encargado del tratamiento.

[997] Así se indica que este documento deberá mantenerse en todo momento actualizado y debe revisarse cuando se produzcan cambios relevantes que puedan afectar al cumplimiento de las medidas de seguridad y también debe adecuarse a la normativa vigente en materia de seguridad de los datos de carácter personal (art. 88, apartados 7 y 8).

Las medidas organizativas tienen como objetivo establecer los roles necesarios y los mecanismos de comunicación y formación que aseguren que todas las personas implicadas en el tratamiento de datos sean conocedoras de las medidas y las cumplan. En este sentido, el responsable debe identificar los usuarios que acceden a los datos y designar al "responsable de seguridad". Los usuarios son las personas o procesos autorizados para acceder a los datos (art. 5.2.p) RLOPD). El responsable de seguridad es una figura propia de la legislación española y que se define como la "persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables" (art. 5.2.l) RLOPD). Es un concepto para este ámbito concreto de las medidas de seguridad, que sólo debe designarse si se debe aplicar el nivel medio de protección.

Es una figura puramente funcional, que pretende servir de instrumento para hacer que se cumplan las medidas de seguridad cuando se manejan datos que merecen una especial protección. Por ello, según la AEPD debería ser una persona con conocimientos suficientes para llevar a cabo estas funciones[998]. Sin embargo, a diferencia del responsable del tratamiento, esta figura no conlleva la atribución de responsabilidad, hecho que se aclara al indicar que la designación de este responsable no supondrá la exoneración de la responsabilidad que corresponda a estos dos sujetos (art. 95 RLOPD).

4. OBLIGACIONES Y DERECHOS RELATIVOS A LA FASE DE SALIDA DE LOS DATOS PERSONALES

4.1. La comunicación de datos

Como ya se ha indicado anteriormente, una característica de la legislación española es la regulación separada de la comunicación de datos. El concepto de cesión o comunicación de datos se encuentra en la LOPD: "toda revelación de datos realizada a una persona distinta del interesado" (art. 3.i) LOPD). De entrada, especialmente el término cesión, nos plantea si estamos ante alguna de las nociones de cesión que establece el derecho civil. Sin embargo, la amplitud del concepto, la adición del término

[998] Informe jurídico de 1999, sin referencia.

"comunicación" y las características específicas del contexto del derecho a la protección de datos hacen que haya que entender que el término adquiere un significado propio[999].

El concepto pone el acento en el acto de revelación de los datos, lo que produce esa ampliación de su alcance. De esta forma, en esta definición no sólo se incluirá el acto mediante el que un sujeto emisor transmite datos a un sujeto receptor, sino también el acto que implica que un emisor ponga a disposición del receptor o receptores los datos, sin tener claro si se llegará a producir la captación de estos por parte de estos sujetos receptores[1000].

La cesión no exige, por tanto, que se incorporen los datos a los ficheros del cesionario y entiendo que no exige tampoco que el cesionario se convierta en responsable del fichero o del tratamiento, respecto a esos datos objeto de la comunicación[1001]. Es decir, no es necesario para que haya cesión de datos que el cesionario tenga capacidad de decidir sobre la finalidad, contenido y uso del tratamiento. Así, se define este destinatario o cesionario como "la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos" y también puede ser "entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados" (art. 5.1.h) RLOPD).

[999] MESSÍA DE LA CERDA BALLESTEROS, tras analizar si se puede asimilar este término "cesión", en el contexto del derecho a la protección de datos, con otras figuras tradicionales del Derecho civil (la cesión de contrato, las estipulaciones a favor de tercero, la asunción de deudas, la cesión de derechos sobre cosa ajena) concluye que no es posible, debido sobre todo a la naturaleza de los datos, un bien inmaterial. Este autor considera que la utilización de este término de cesión debe calificarse de desafortunada, precisamente por la confusión respecto a estas otras figuras, si bien al añadir el término "comunicación" se consigue alejar la noción de estos conceptos. J.A. MESSÍA DE LA CERDA BALLESTEROS, *La Cesión o comunicación de datos de carácter personal*, Aranzadi, Cizur Menor (Navarra), 2003, págs. 51 a 61.

[1000] Así, por ejemplo, cuando se publica una lista sin incluir ningún tipo de restricción de datos en Internet, se pone a disposición de un grupo indeterminado de sujetos receptores la información. *Ibídem*, págs. 58 a 59.

[1001] El Tribunal Supremo sostiene que el artículo 3.i) LOPD "no contempla, en la definición que ofrece de cesión o comunicación de datos, la necesidad o requisito de que la revelación vaya acompañada de una entrega material de los datos ni, por supuesto, de una incorporación al fichero del cesionario. Lo único que exige el precepto legal es la acción de revelar, esto es, la de hacer saber cosas que se mantenían ocultas, sin requerir que tal forma de proceder revista una forma determinada. Si se exigiera, como erróneamente sostiene la recurrente, una entrega material de los datos y su incorporación al fichero del cesionario, mal podría sostenerse que la Ley responde al principio general que recoge su artículo 1 y que señala como objetivo de la misma, en absoluta armonía con el artículo 1.1 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1998, "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente en su honor e intimidad personal y familiar"." STS de 17 de septiembre de 2010 (Sala 3ª) (ROJ: STS 4940/2010), FJ 5.

Sin embargo, evidentemente deberá entenderse aplicable la regulación del derecho a la protección de datos, ya que la cesión se considera una modalidad de tratamiento de datos[1002]. Así se confirma con el concepto de cesión o comunicación de datos que establece el RLOPD que únicamente contiene un matiz diferente, respecto a la definición mencionada de la LOPD, matiz que clarifica que estamos ante un tratamiento de datos[1003]. Si además se acude a la definición de tratamiento de datos que estipula el mismo RLOPD en su última parte se alude a "las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias" (art. 5.1.t RLOPD), alusión que permanece idéntica a la que podemos encontrar en la LOPD en su definición de tratamiento de datos (art. 3.c LOPD). De esta definición de tratamiento de datos se puede deducir la naturaleza eminentemente técnica del término cesión o comunicación de datos que lo que pretende es incorporar cualquier forma de transmisión de datos.

De todo lo anterior se concluye que la cesión se producirá con la simple divulgación de los datos, aunque estos luego no sean incorporados en un fichero y aunque quien pueda acceder a los mismos no cumpla con los requisitos establecidos para ser un responsable del tratamiento o del fichero. La protección del derecho vendrá, por tanto, de la posición de quien cede los datos, de quien los revela, quien, al llevar a cabo esta cesión, sin duda, se configurará como un responsable que decide al respecto de este tratamiento[1004]. En cuanto a la responsabilidad que pueda tener el sujeto cesionario, ello dependerá de la conducta que realice.

4.1.1. La regulación específica de la cesión de datos

El artículo 11 LOPD es el precepto que establece la regulación de la cesión de datos en el marco de las disposiciones generales, por lo que se aplicará a todo tipo de ficheros (de titularidad pública y privada). Asimismo, como también se ha indicado, es preciso tener en cuenta el artículo 10 RLOPD que incorpora los supuestos legitimadores del tratamiento o cesión de los datos y la regulación del RLOPD referida a la obtención del consentimiento del afectado (especialmente art. 12.2 RLOPD) y a las notificaciones

[1002] STS de 17 de septiembre de 2010 (Sala 3ª) (ROJ: STS 4940/2010), FJ 5, que afirma categóricamente que la cesión es una modalidad de tratamiento.
[1003] Así se define cesión o comunicación de datos como "tratamiento de datos que supone su revelación a una persona distinta del interesado" (art. 5.1.c RLOPD).
[1004] Así lo entiende también J.A. MESSÍA DE LA CERDA BALLESTEROS, *La Cesión o comunicación de datos de carácter personal*, *op. cit.*, págs. 61 a 62.

que el responsable debe realizar a los cesionarios relativas a la revocación del consentimiento y al ejercicio de los derechos ARCO.

Se establecen los siguientes requisitos para poder comunicar datos: el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario y el previo consentimiento del interesado (art 11.1 LOPD). Con la primera exigencia se pretenden evitar las cesiones que no se incluyan en la esfera de las relaciones entre las partes (cedente y cesionario), por lo que no cabría una cesión, cuyo único objetivo fuera la misma cesión, sino que debería incardinarse en estas relaciones, revistiendo, por tanto, un carácter instrumental[1005].

La AEPD aplica este primer requisito relativo al cumplimiento de fines relacionados con las funciones legítimas de cedente y cesionario, especialmente, cuando se plantea la aplicación del interés legítimo como base jurídica para poder realizar el tratamiento de datos. La legitimación del cesionario fundamentada en el interés legítimo se condiciona a que el tratamiento realizado por el cedente fuera legítimo, ya que si no fuera así, esta falta de legitimación del cedente contaminaría la del cesionario[1006]. De esta forma, la AEPD obliga al cesionario a realizar un control de la legitimación del cedente[1007]. Esta conexión entre ambas legitimaciones no parece acorde con la dicción del RLOPD ni de la Directiva 95/46/CE, que establecen la conjunción disyuntiva "o" en este supuesto de legitimación: "el tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparados por dichas normas" (art. 10.2.a) RLOPD). Ello sin perjuicio de la existencia de supuestos de

[1005] MESSÍA DE LA CERDA BALLESTEROS planteaba si este requisito suponía que no se aplicara el principio de finalidad del artículo 4 LOPD, lo que descarta, al entender que los principios contenidos en este artículo son principios de la protección de datos que deben aplicarse a todos los tipos de tratamiento, incluyendo también las cesiones. J.A. MESSÍA DE LA CERDA BALLESTEROS, *La Cesión o comunicación de datos de carácter personal*, *op. cit.*, págs. 99, 103.

[1006] En una consulta planteada a la AEPD sobre la aplicación del supuesto de legitimación relativo al interés legítimo, tras la Sentencia del TJUE de 24 de noviembre de 2011, *ASNEF, FECEMD/Administración del Estado*, la AEPD indica que "la legitimación del cesionario fundada en su interés legítimo sólo será posible si es legítimo el tratamiento llevado a cabo por su cedente, de forma que en caso de que el tratamiento sea ilícito en origen la mera invocación de un interés legítimo, aun cuando resulte prevalente, por el cesionario de los datos no implica que ese tratamiento devenga legítimo, por cuanto los datos habrían sido ilegítimamente sometidos a tratamiento en origen.". Informe 111/2012 de la AEPD.

[1007] Cabe preguntarse el alcance de ese control de legitimación. Es decir, la AEPD obliga al cesionario a asegurarse de que el cedente ha cumplido con todos los requisitos que establece la normativa de protección de datos, como el deber de informar. Sin embargo, si lo que se analiza es la legitimación y si aceptamos la interpretación de la AEPD ¿no debería ser sólo ese aspecto el que debería controlar el cesionario?

corresponsabilidad, donde podrá delimitarse la responsabilidad de cada uno de los responsables.

4.1.2. El consentimiento y sus excepciones

El reconocimiento de la relevancia constitucional del consentimiento que se comentaba en sede de legitimación, debe extenderse al consentimiento para la cesión de datos, que también es imprescindible para atribuir el control sobre sus datos al titular del derecho[1008]. Asimismo, para conocer los requisitos del consentimiento hay que remitirse a lo explicado respecto al consentimiento para poder tratar datos personales, ya que tendrá las mismas características con sólo una diferencia: que en este caso se añade el adjetivo "previo". No obstante, el RLOPD se ocupa de añadir también este adjetivo para todo supuesto de tratamiento de datos y no sólo para la cesión (art. 10.1 RLOPD). El consentimiento también será revocable (art. 11.4 LOPD), al igual que sucedía con el consentimiento general para tratar datos[1009].

Se establece la nulidad del consentimiento, si la información que se facilite al interesado no le permite conocer la finalidad a que destinarán los datos, cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar (art. 11.3 LOPD). Esta previsión se repite en el RLOPD aunque redactado en positivo (art. 12.2 RLOPD). Así, a diferencia de lo que sucedía en la LORTAD, que exigía que el cesionario fuese determinado o determinable, en la LOPD no se exige esta determinación, excepto en el caso de los ficheros de titularidad privada, como comentaremos[1010]. En este sentido, la STC 292/2000, de 30 de septiembre indicaba que:

> "el interesado debe ser informado tanto de la posibilidad de cesión de sus datos personales y circunstancias como del destino de éstos, pues sólo así será eficaz su derecho a consentir" "Para lo que no basta que conozca que tal cesión es posible según la disposición que ha creado o modificado el fichero, sino también las circunstancias de cada cesión concreta", STC 292/2000, de 30 de septiembre de 2000, FJ 13.

[1008] STC 292/2000, de 30 de noviembre de 2000, FJ 7.
[1009] Si bien no se especifica al igual que sucedía en el consentimiento general para tratar datos el hecho de que la revocación no tenga efectos retroactivos, aunque debe entenderse que también se aplicará a este caso de la cesión. Asimismo, cabe aplicar la regulación que el art. 17 RLOPD establece para llevar a cabo la revocación del consentimiento.
[1010] J.A. MESSÍA DE LA CERDA BALLESTEROS, *La Cesión o comunicación de datos de carácter personal*, *op. cit.*, pág. 59.

La LOPD ha considerado que las circunstancias concretas de la cesión no incluyen la identidad del cesionario en todos los casos. Sin embargo, no parece acorde con la obligación de informar sobre los destinatarios el hecho de no individualizarlos (art. 5.1.a) LOPD).

Las excepciones al requisito del consentimiento (que no al relativo al cumplimiento de fines directamente relacionados con las funciones legítimas de cedente y cesionario) son, según su redacción en la LOPD:

> "a) Cuando la cesión está autorizada en una ley b) Cuando se trate de datos recogidos de fuentes accesibles al público c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique; d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica." (art. 11.2 LOPD).

El primer supuesto para el que no será preciso el consentimiento del interesado es cuando lo autorice una ley. En este sentido, el RLOPD especifica que debe tratarse de una norma con rango de ley o una norma de derecho comunitario (10.2.a RLOPD). Además se aclara en el RLOPD que pueden darse dos supuestos: cuando la cesión tenga por objeto la satisfacción de un interés legítimo del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 LOPD o cuando la cesión sea necesaria para que el responsable del tratamiento cumpla con un deber que le imponga una de dichas normas.

Estas precisiones responden a las cuestiones que se planteaban en torno a si era necesario que apareciese estipulado de forma expresa esta cesión en las normas. De esta forma, queda claro que basta con que la cesión se precise para que el responsable cumpla un deber que sí esté previsto expresamente en las leyes o que sea para la satisfacción de un interés legítimo, si no prevalece el interés o los derechos y libertades de los interesados.

En lo que respecta al supuesto de la letra b), que se refiere a cuando los datos estén recogidos en fuentes accesibles al público, me remito a los comentarios realizados respecto a la sentencia de 24 de noviembre de 2011 del TJUE, que estableció la incorrecta transposición del artículo 7.f) Directiva 95/46/CE por la legislación española y, más concretamente, por el artículo 10.2.b RLOPD[1011]. Este precepto del RLOPD, anulado por el Tribunal Supremo[1012], incluía dos supuestos equivalentes de legitimación del tratamiento y la cesión (los ubicados en los arts. 6.2 in fine y 11.2.b) LOPD). Por tanto, entiendo que este precepto también debe quedar sustituido por la aplicación directa del artículo 7.f) Directiva 95/46/CE. El hecho de que los datos estén incluidos en fuentes accesibles al público debe quedar como un criterio a tener en cuenta en la ponderación a realizar, tal como señalaba el TJUE[1013].

Respecto al supuesto de la letra e) relativo a la comunicación entre administraciones públicas, también hay que tener en cuenta lo establecido en el artículo 21 LOPD, al que se hará referencia a continuación.

4.1.3. La cesión de datos en el marco de los ficheros de titularidad pública

En la LOPD se incluye una regulación específica sobre la comunicación de datos en ficheros de titularidad pública en el artículo 21 LOPD, que fue parcialmente anulado por la STC 292/2000, de 30 de noviembre de 2000, y su redacción final no permite que se comuniquen datos entre administraciones públicas para el ejercicio de competencias diferentes o de competencias sobre materias distintas, salvo que la comunicación tenga

[1011] Sentencia del TJUE de 24 de noviembre de 2011, *ASNEF, FECEMD/Administración del Estado*, C-468/10 y C-469/10, EU:C:2011:777.
[1012] STS de 8 de febrero de 2012 (Sala 3ª) (ROJ: STS 429/2012).
[1013] Sentencia del TJUE de 24 de noviembre de 2011, *ASNEF, FECEMD/Administración del Estado*, C-468/10 y C-469/10, EU:C:2011:777, apdos. 44 y 45. También se ha manifestado la AEPD en este sentido en los informes que ha emitido sobre algunas consultas relativas a esta cuestión, como el Informe AEPD 111/2012. De esta forma, si los datos tratados por el responsable para la satisfacción de su interés legítimo se han obtenido de fuentes accesibles al público, será más fácil *a priori* que hagan que prime este interés del responsable sobre el de los interesados. Además la AEPD cita en sus informes la SAN de 31 de mayo de 2012 (Sala de lo contencioso-administrativo) (ROJ: SAN 2747/2012), FJ 3, que también especifica que el hecho de que los datos figuren o no en fuentes accesibles al público debe tomarse como un elemento más de ponderación.

por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos[1014].

Este precepto específico para los ficheros de titularidad pública también prohíbe la comunicación de datos recogidos de fuentes accesibles al público a ficheros de titularidad privada, a no ser que se cuente con el consentimiento del interesado o cuando una ley prevea otra cosa (art. 21.3 LOPD).

En definitiva, para mayor claridad, se recogieron en el RLOPD los supuestos que permitían la cesión sin consentimiento en este ámbito, de forma que serían: cuando sea con fines históricos, estadísticos o científicos, cuando una administración pública obtenga o elabore los datos con destino a otra y cuando sea para el ejercicio de competencias idénticas o que versen sobre las mismas materias (art. 10.4.c) RLOPD).

Hay que decir que, respecto a las comunicaciones en el ámbito de las administraciones públicas, parte de la doctrina interpreta que los accesos que realizan a los datos los diferentes departamentos de la misma administración no se consideran comunicación[1015]. Aunque el criterio de la personalidad jurídica no se utilice para

[1014] Se resume lo manifestado por el Tribunal Constitucional con lo siguiente: "El motivo de la inconstitucionalidad del art. 21.1 LOPD resulta, pues, claro. La LOPD en este punto no ha fijado por sí misma, como le impone la Constitución (art. 53.1 CE), los límites al derecho a consentir la cesión de datos personales entre Administraciones Públicas para fines distintos a los que motivaron originariamente su recogida, y a los que alcanza únicamente el consentimiento inicialmente prestado por el afectado (art. 11 LOPD, en relación con lo dispuesto en los arts. 4, 6 y 34.e LOPD), sino que se ha limitado a identificar la norma que puede hacerlo en su lugar. Norma que bien puede ser reglamentaria, ya que con arreglo al precepto impugnado será una norma de superior rango, y con mayor razón para el caso de que la modificación lo sea por una norma de similar rango, a la que crea el fichero (y ésta basta con que sea una disposición general, que no una Ley, publicada en un Boletín o Diario oficial —art. 20.1 LOPD) la que pueda autorizar esa cesión inconsentida de datos personales, lo que resulta ser, desde luego, contrario a la Constitución." STC 292/2000, de 30 de noviembre de 2000, FJ 14.

[1015] Así lo consideran A. TRONCOSO REIGADA, *La protección de datos personales. En busca del equilibrio*, *op. cit.*, págs. 440 a 452 y A. CERRILLO I MARTÍNEZ, "Comunicación de datos entre administraciones públicas", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, págs. 1.308 a 1.311. También parece seguir esta postura la ACPD que, ante una consulta relativa a si se podían entregar datos personales a los concejales de un ayuntamiento consideró que los concejales de un ayuntamiento, al ser parte integrante del ayuntamiento, no eran un tercero ajeno a la relación entre el interesado (el titular de los datos) y el propio ayuntamiento, por lo que no habría comunicación de datos, sino un acceso a los datos que debería limitarse en función del principio de calidad. Dictamen CNS 13/2007 de la ACPD. Asimismo, la ACPD indica que "las transmisiones de datos entre órganos que forman parte de una misma administración no se consideran comunicación de datos" en su Recomendación 1/2010 de la *Agència Catalana de Protecció de Dades*, sobre el encargado de tratamiento en la prestación de servicios por cuenta de entidades del sector público de Cataluña, apdo. 16. En cambio, la AEPD ha calificado de cesión de datos la transmisión de datos del ayuntamiento a un concejal en su Informe 0016/2010.

identificar a los responsables, ya que, como se comentó, en la definición queda claro que podrán ser responsables los órganos administrativos, sí que se utiliza, en este caso, para identificar si hay cesión o no. De esta forma, sólo cuando la transmisión de datos se efectúe entre administraciones con personalidad jurídica diferenciada, se entenderá que existe cesión. Como indican quienes defienden esta postura, la protección vendrá garantizada por el principio de calidad.

4.1.4. La cesión de datos en el marco de los ficheros de titularidad privada

El artículo 27 LOPD, ubicado en el Título IV, dedicado a las disposiciones sectoriales y en su Capítulo II, donde se encuentra la regulación de ficheros de titularidad privada, establece:

> "Comunicación de la cesión de datos. 1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario. 2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por la ley" (art. 27 LOPD).

Este precepto regula un deber específico de información para el momento en que el responsable del fichero efectúe la primera cesión de datos. Respecto al contenido de este deber de información, la mención a los datos "cedidos" parece dar a entender que se trata de un deber de información *a posteriori*, cuando ya se haya producido la cesión. No obstante, al indicarse que el responsable del fichero debe llevarlo a cabo "en el momento en que se efectúe la primera cesión de datos", apunta más bien a una información previa. Otro aspecto que resulta confuso es lo que significa la referencia a la primera cesión. Si posteriormente se realizan otras cesiones de datos del mismo interesado al mismo cesionario, deberá cumplirse también este deber de información. ¿Y si las cesiones son a otros cesionarios?

Se podría decir que estamos ante el artículo "olvidado", ya que prácticamente no se hallan ejemplos de su aplicación por parte de la AEPD. Los tribunales y también la doctrina han abordado en contadas ocasiones su análisis, y en el último caso, desde una

visión crítica[1016]. Sin duda, ello se debe a que se trata de una disposición incómoda, de cumplimiento harto complicada y que, hasta hace bien poco, no constituía una sanción evidente para el responsable.

No puede alabarse la inclusión de este precepto en la LOPD. Copiado de forma mimética del artículo 25 LORTAD, este artículo tiene su origen en la Propuesta de Directiva de 1990. Como ya se ha señalado en este trabajo, esta propuesta inicial de la Directiva 95/46/CE sirvió de inspiración, en algunos casos como este, de forma exagerada, a la LORTAD. A su vez, la Propuesta de Directiva de 1990 incorporó un precepto de la Ley federal alemana de 1990[1017]. Esta cadena de traslaciones de una ley a la otra distorsionó el sentido del precepto, hasta dar como resultado el artículo 27 LOPD.

[1016] Como ejemplo de esta doctrina cabe citar a APARICIO SALOM, muy crítico con esta disposición, que la califica de "totalmente incomprensible" y expresa su sorpresa de que se haya mantenido en la LOPD, pese a las críticas que se habían realizado y el hecho de que la propia AEPD no hubiera exigido el cumplimiento de la misma. J. APARICIO SALOM, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*. 3ª Ed., Aranzadi, Elcano, 2009, págs. 233 a 235. Respecto a las sentencias sólo he podido hallar dos en las que se aplique el art. 27 LOPD, ambas de la Audiencia Nacional: SAN de 13 de abril de 2005 (Sala de lo contencioso-administrativo) (ROJ: SAN 6741/2005) y SAN de 21 de septiembre de 2005 (Sala de lo contencioso-administrativo) (ROJ: SAN 4494/2005).

[1017] La Propuesta de Directiva de 1990, en su artículo 9.1, establecía bajo el título "obligación de información al interesado": "Por lo que se refiere al sector privado, los Estados miembros dispondrán en su legislación que en el momento de la primera comunicación o cuando se plantee la posibilidad de consulta en línea, el responsable informe de ello al interesado y le indique asimismo la finalidad del fichero, el tipo de datos que contiene y su nombre y dirección". En su apartado 2 excluía del cumplimiento de esta obligación al supuesto establecido en el artículo 8.1.b), es decir, cuando los datos se hubieran obtenido de fuentes accesibles al público y su tratamiento se dedicara, únicamente, a fines de correspondencia, y cuando la comunicación estuviera prevista en una ley. Además, en su apartado 3 se establecía que, si el interesado objetaba a la comunicación o a cualquier otro tratamiento, el responsable del fichero debería cesar en el tratamiento objetado, a no ser que estuviera autorizada su ejecución por ley. Este precepto, a su vez, se inspiraba en el parágrafo 33 de la Ley federal alemana de 1990 que disponía: "Si se almacenaren por primera vez datos personales para los fines propios del almacenante, el afectado será informado de oficio del hecho del almacenamiento y de la naturaleza de los datos almacenados. Si se almacenaren datos personales para la gestión ordinaria con el propósito de cederlos, el afectado será informado de oficio de la primera cesión y de la naturaleza de los datos almacenados." El párrafo segundo preveía excepciones si el afectado hubiera conocido por otra vía el almacenamiento o la cesión, o si el almacenamiento estuviera impuesto por ley o por contrato, si los datos tuvieran que ser mantenidos en secreto o si el almacenamiento fuera transitorio y no excediera de tres meses. Como se puede observar, el artículo 9 de la Directiva 95/46/CE modifica este precepto del que se inspira, de forma que quedaría parcialmente recogido, ya que no distingue entre los dos supuestos que diferenciaba la Ley federal alemana. Esta ley contemplaba la obligación de informar cuando se produjera la primera cesión de datos, sólo en el supuesto en el que se almacenaran datos para la gestión ordinaria con el propósito de cederlos, lo que se diferenciaba del supuesto en el que se almacenaba por primera vez datos, se entiende que refiriéndose a cuando se recaban los mismos directamente del interesado. El debate parlamentario durante la elaboración de la LORTAD refleja que los diputados sólo se preocuparon de que el precepto trasladara de la forma más fiel posible el artículo de la Propuesta de Directiva de 1990. M. HEREDERO HIGUERAS, *La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (Comentarios y textos)*, Tecnos, Madrid, 1996, págs. 178 a 180.

Por otro lado, la Directiva 95/46/CE sufrió un proceso largo de tramitación, por lo que la Propuesta de Directiva de 1990, en la que se encontraba esta disposición, varió bastante hasta llegar a la versión final de 1995. Si bien se mantiene la alusión a la información, en el momento de la primera cesión de datos, se establece en los casos en que los datos no se recaben directamente del titular de los datos. En este caso, se estipula que, si se piensa comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos, deberá informarse al interesado obligatoriamente de la identidad del responsable y, en su caso, de su representante y de los fines del tratamiento (art. 11.1 Directiva 95/46/CE). Asimismo, se podrá establecer la necesidad de que el responsable informe de otros aspectos opcionales (categorías de datos, destinatarios, derechos de acceso y rectificación de los datos), en la medida en que, habida cuenta de las circunstancias en que se hayan obtenido los datos, fuera necesaria para garantizar un tratamiento de datos leal. No deberá cumplirse con esta obligación si el interesado ya hubiera sido informado de los aspectos obligatorios. También hay que recordar que se establecen algunas excepciones a esta obligación (art. 11.2 Directiva 95/46/CE).

En el preámbulo de la Directiva 95/46/CE se justifica que, en el caso de que el responsable no haya recogido los datos directamente del interesado o si en el momento de la recogida no hubiera previsto la comunicación a terceros de los datos, es comprensible que, de todas formas, pueda realizar comunicaciones (Considerando 39 Directiva 95/46/CE). No obstante, para hacerlo, el responsable deberá informar al interesado, en el momento del registro de los datos o al comunicarse los datos por primera vez al tercero.

Por tanto, el artículo 27 LOPD no se ajusta a esta regulación de la Directiva 95/46/CE, ya que sólo se refiere a ficheros de titularidad privada y se aplica, tanto a datos recogidos de forma directa, como indirecta. No establece tampoco que se pueda evitar su cumplimiento si ya se ha informado de los aspectos relacionados en el mismo. Sin embargo, el precepto establece algunos casos en los que no se exigirá su cumplimiento y que son prácticamente todos aquellos que suponen excepciones a la necesidad de solicitar consentimiento para poder comunicar datos previstos en el artículo 11 LOPD[1018].

[1018] Estos supuestos son los establecidos en los apartados 2, letras c), d), e) y 6 del artículo 11 LOPD: cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros, cuando la comunicación deba efectuarse al Defensor del Pueblo, al Ministerio Fiscal, Jueces, Tribunales o Tribunal de Cuentas, en el ejercicio de las funciones que tienen atribuidas, cuando la cesión se produzca

Por lo tanto, cuando se exija el consentimiento previo para comunicar datos (y siempre que estemos ante ficheros de titularidad privada) será necesario también cumplir con este específico deber de información, mucho más estricto que el que se requiere para cumplir con el requisito del consentimiento en caso de cesión de datos. Como ya se ha visto, para que este consentimiento sea válido no es necesario identificar al concreto cesionario, sino que basta con identificar la actividad desarrollada por el mismo y la finalidad a la que se destinarán los datos. En cambio, el artículo 27 LOPD sí exige esta identificación (nombre y dirección) y además que se informe de la naturaleza de los datos cedidos.

La única lógica que podría tener esta regulación es que, cuando se exige el consentimiento para comunicar datos personales no se tuviera la información exacta de quien iba a ser el cesionario concreto y bastara con indicar la actividad del mismo. La obligación de identificar concretamente a este cesionario se retrasaría hasta el momento de realización de la cesión, momento en el que ya se contaría con esa información. Pero en este caso, el consentimiento no tendría eficacia hasta que no se hubiera cumplido con esta identificación, pero ¿por qué establecer esta restricción sólo para ficheros de titularidad privada?

Por otro lado, si el deber de información es posterior a la cesión, se solaparía con la obligación de información que tendría el responsable cesionario de estos datos de informar, entre otros aspectos, de la procedencia de los datos (art. 5.4 LOPD). Es cierto que, en este caso, el cesionario quedaría exonerado de cumplir con este deber si el interesado ya hubiera sido informado previamente. Sin embargo, tampoco el cumplimiento del artículo 27 LOPD permitiría a este cesionario librarse del cumplimiento

---

entre administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos, cuando la comunicación se realice previo procedimiento de disociación y también cuando la cesión venga impuesta por ley. El supuesto de cesión entre Administraciones públicas parece obvio, ya que estamos en sede de ficheros de titularidad privada y no cabría, por tanto, cumplir este precepto en este caso. No obstante, para FERNÁNDEZ SALMERÓN esta remisión implica que se aplique este precepto a otras cesiones entre administraciones públicas en las que no concurran los fines históricos, estadísticos o científicos. Así, salvo cuando la cesión interadministrativa venga impuesta por ley, la administración cedente, según el autor, deberá proceder según lo preceptuado en el artículo 27 LOPD. M. FERNÁNDEZ SALMERÓN, *La protección de los datos personales en las Administraciones Públicas*, Civitas, Madrid, 2003, págs. 303 a 304.

de su deber de información, ya que no encajan exactamente, en los dos preceptos implicados, los aspectos que conforman el contenido del que debe informarse.

Otro aspecto muy importante a tener en cuenta, en la aplicación del artículo 27 LOPD, es el cuadro sancionador que establece la LOPD, para el incumplimiento de este artículo. Hasta la modificación de este marco sancionador en el año 2011[1019], la LOPD establecía infracciones referidas al incumplimiento del deber de información, pero no se incluía este artículo 27 LOPD entre los que podían originar estas infracciones[1020]. Si bien es cierto, que la falta de sanción no debe implicar la impunidad en caso de incumplimiento, al tratarse de un precepto de naturaleza imperativa, lo cierto es que no era posible que la AEPD pudiera sancionar esta conducta, al no contar con la tipificación adecuada[1021].

[1019] Modificación de los artículos 43, 44, 45, 46 y 49 LOPD, introducida por la Ley 2/2011 de 4 de marzo de Economía Sostenible (BOE núm. 55, de 5 de marzo de 2011, págs. 25033-25235). Ver Capítulo VII.

[1020] Se establecía concretamente como infracción de tipo leve en su artículo 44.2.d) LOPD "proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley". Era infracción de tipo grave que establecía el artículo 44.3.l) LOPD "incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado". Asimismo se sancionaba como infracción muy grave en su artículo 44.4.b) "la comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.".

[1021] La AEPD lo intenta sin éxito en un asunto, en el que la Audiencia Nacional estima el recurso contencioso-administrativo interpuesto por el BBVA y anula la resolución del Director de la AEPD, que había impuesto una sanción de multa de 60.101,21 € a esta entidad. El supuesto, relativo a una cesión de créditos que había efectuado la entidad recurrente a otra entidad financiera, implicó la denuncia, por parte de uno de los prestatarios, que alegaba que no se le había informado de esta cesión. La AEPD entendió que se trataba de una cesión inconsentida que infringía el artículo 11 LOPD y el artículo 27 LOPD. La AEPD acudió al artículo 27 LOPD porque la infracción relativa a la cesión que se establecía en el artículo 44.4.b) LOPD había prescrito al haber transcurrido más de tres años, plazo de prescripción de las infracciones muy graves. En cambio, la AEPD consideró que la infracción originada por la vulneración del artículo 27 LOPD era una infracción continuada, que se sancionaba por la infracción grave descrita en el artículo 44.3.d) LOPD, que establecía "tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidas en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituye infracción muy grave". La Audiencia Nacional no acepta este encaje, ya que considera que el artículo 27 LOPD contempla un deber de información, que no puede encuadrarse en el tipo sancionador, que lo que contempla es una acción de tratamiento o utilización. Además, el artículo 44.3.d) LOPD establece un principio de subsidiaridad, en virtud del que sólo entrará en juego, cuando no pueda considerarse infracción muy grave el supuesto, que en este caso se había calificado así por la AEPD pero, como se ha indicado, no pudo ser sancionado en virtud del instituto de la prescripción. SAN de 21 de septiembre de 2005 (Sala de lo contencioso-administrativo) (ROJ: SAN 4494/2005), FJ 4. También se puede mencionar otra sentencia de la Audiencia Nacional que desestima el recurso de una compañía de seguros que había sido sancionada por la AEPD por haber cedido la cartera de clientes sin haber solicitado consentimiento. Pese a que se menciona el incumplimiento del artículo 27 LOPD, la AEPD alega la vulneración del artículo 11 LOPD. SAN de 13 de abril de 2005 (Sala de lo contencioso-administrativo) (ROJ: SAN 6741/2005), FJ 2. MESSÍA DE LA CERDA BALLESTEROS indica que la falta de sanción no implicaba la impunidad de este incumplimiento del artículo 27 LOPD, ya que al tratarse de un precepto de naturaleza imperativa el acto contrario al mismo, por aplicación del artículo 6.3 Cc resultaría nulo. J.A. MESSÍA DE LA CERDA BALLESTEROS, *La Cesión o comunicación de datos de carácter personal, op. cit.*, pág. 109.

Con el nuevo marco sancionador se abren nuevas posibilidades para el, hasta ahora, denostado artículo 27 LOPD. Y es que las infracciones relativas al cumplimiento del deber de información ya no se remiten a artículos concretos, sino que se refieren al incumplimiento del deber de información al afectado, cuando los datos sean recabados del propio interesado (art. 44.2.c) LOPD) y al incumplimiento del deber de información, cuando los datos no hayan sido recabados del propio interesado (art. 44.3.f) LOPD). Si bien es cierto que estas infracciones parece que claramente se refieren al incumplimiento del deber de información general (art. 5 LOPD), podrían dar cabida a este artículo 27 LOPD. También podría ser posible encuadrar el incumplimiento de este precepto, en la infracción relativa al incumplimiento de los restantes deberes de notificación o requerimiento al afectado, impuestos por esta ley y sus disposiciones de desarrollo (art. 44.3.g) LOPD).

4.1.5. La cesión de datos especialmente protegidos

Cuando lo que se pretende comunicar son datos especialmente protegidos, no se podrá aplicar automáticamente la regulación general (art. 11 LOPD), sino que se tendrá en cuenta la regulación específica de este tipo de datos (arts. 7 y 8 LOPD). La aplicación en estos casos de esta regulación específica se confirma en el RLOPD (art. 10.5 RLOPD), con un afán más que nada divulgativo, debido a la tendencia a aplicar erróneamente la regulación general de las cesiones[1022].

En definitiva, en el caso de datos que revelen la ideología, afiliación sindical, religión y creencias, sólo podrán cederse si se cuenta con el consentimiento expreso y por escrito del afectado (art. 7.2 LOPD)[1023]. Si son datos referidos al origen racial, a la salud y a la vida sexual sólo podrán cederse cuando, por razones de interés general, así lo

[1022] Y es que la confusión sobre el precepto aplicable, en estos supuestos, se ve favorecida por la referencia, que el mismo artículo 8 LOPD -que regula específicamente los datos de salud- hace al artículo 11 LOPD: "Sin perjuicio de lo dispuesto en el artículo 11 respecto de la cesión[…]" que apunta a un supuesto en este precepto que se refiere a los datos de salud (el art. 11.2.f) LOPD). Se trata de uno de los efectos desfavorables del mantenimiento en nuestra normativa de una regulación diferenciada para la cesión respecto al resto de operaciones de tratamiento.

[1023] Hay que puntualizar que este requisito se establece para poder tratar estos datos, sin hacer mención a la cesión (art. 7.2 LOPD). Sin embargo, cuando se establece la excepción que permite el tratamiento de datos a partidos políticos y otras entidades de índole política y religiosa, respecto a sus miembros, se especifica que no podrá aplicarse la excepción a la cesión de estos datos. Por ello, hay que entender que será posible la cesión en general si se cuenta con el consentimiento expreso y por escrito.

disponga una ley o el afectado consienta expresamente (art. 7.3 LOPD). No obstante, también hay que tener en cuenta la excepción en el ámbito de los datos de salud tratados por instituciones, centros sanitarios y profesionales del sector (arts. 8 LOPD y 10.5 RLOPD)[1024]. Asimismo, hay que referirse a la excepción que se contemplaba en la regulación general relativa a los datos de salud que podían cederse si ello fuera necesario para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad (art. 11.2.f) LOPD).

La regulación diferenciada de la cesión implica que nos cuestionemos qué sucede en los casos en los que se permite el tratamiento de datos especialmente protegidos, pero no se hace mención de la cesión de forma expresa. Esto sucede en el caso de los tratamientos permitidos de estos datos para la prevención o el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios (art. 7.6 LOPD) o para fines policiales (art. 22 LOPD). Si atendemos a esa especial regulación diferenciada, en estos casos se deberían aplicar los requisitos generales que establecen los preceptos comentados (arts. 7.2 y 7.3 LOPD).

4.2. El encargo del tratamiento

El encargo del tratamiento se regula en el artículo 12 LOPD (desarrollado en los arts. 20 a 22 RLOPD) y se ubica en la parte general, en los principios de protección de datos. La rúbrica de este precepto -acceso a los datos por cuenta de terceros- no puede sino calificarse de desafortunada, al denominar al responsable "tercero", ya que se refiere al acceso que el encargado realiza a los datos personales por cuenta del responsable. Seguramente, esta es la razón de que a esta disposición la doctrina la conozca por la figura del encargado del tratamiento, protagonista del precepto.

El encargo del tratamiento se establece con el fin de regular aquellos supuestos en los que el responsable contrata los servicios de un tercero, que exigen para su desarrollo, que este tercero trate datos de carácter personal, que forman parte de un tratamiento o de

[1024] Se concreta de este modo en el mencionado art. 10.5 RLOPD la posibilidad de comunicar datos de salud, "incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para al atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud".

un fichero del que ostenta la cualidad de responsable el cliente. De esta forma, se pretende con esta regulación posibilitar esta contratación, sin que se pierdan las garantías de protección de los datos que exige la normativa.

Ya se realizó una aproximación al concepto de encargado del tratamiento y su delimitación con el de responsable, cuestión que, en ocasiones es sumamente compleja[1025]. Una vez se determina que un sujeto actúa en calidad de encargado del tratamiento, hay que analizar si se cumplen las garantías establecidas en la legislación para esta figura. Sólo si se cumplen los requisitos se podrán acoger responsable y encargado a esta especial regulación.

4.2.1. La configuración del régimen del encargo

Como se ha visto, la cesión de datos es una operación de tratamiento de datos que tiene, a diferencia de lo que sucedía en la Directiva 95/46/CE, una regulación específica y diferenciada en la normativa española. La figura del encargo del tratamiento se configura en la legislación española como una ficción jurídica que establece que el acceso a datos, en estos supuestos, no será considerado comunicación, pese a que materialmente se trate de una transmisión de datos de un sujeto a otro[1026]. Por tanto, no será aplicable a estos casos la regulación de las cesiones de datos, que establece como principio general la exigencia de consentimiento[1027]. No obstante, para que la ficción produzca sus efectos deberán cumplirse las garantías establecidas en la regulación de forma estricta. Si no se cumple con estas garantías se entenderá que la ficción jurídica desaparece y se aplicará la regulación general, por lo que se producirá un incumplimiento. No hay que olvidar que el encargado del tratamiento, junto con el responsable, son las dos únicas figuras que en la legislación española están sujetas al cuadro sancionador de la LOPD y al régimen de responsabilidad[1028].

[1025] Ver Capítulo III.
[1026] STS de 4 de mayo de 2009 (Sala 3ª) (ROJ: STS 2651/2009), FJ 2 y J. RUBÍ NAVARRETE, "El encargado del tratamiento", A. PALOMAR OLMEDA, P. GONZÁLEZ ESPEJO (dirs.); C. ÁLVAREZ RIGAUDIAS (Coord.), VVAA, *Comentario al Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal: (aprobado por RD 1720/2007, de 21 de diciembre)*, Aranzadi, Cizur Menor (Navarra), 2008, pág. 216.
[1027] No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento (art. 12.1 LOPD).
[1028] Ver Capítulo VII.

4.2.2. La relación contractual entre responsable y encargado del tratamiento

La LOPD exige que el acceso a los datos debe ser necesario para la prestación de un servicio al responsable del tratamiento (art. 12.1 LOPD). Por tanto, debe existir una necesidad que debe valorar el responsable del tratamiento, de forma que sólo permita el acceso a los datos personales si ello es preciso[1029]. Asimismo, esta necesidad debe enlazarse con el principio de calidad que exige que sólo se traten los datos adecuados, pertinentes y no excesivos para la finalidad del tratamiento y, por tanto, deberán limitarse los datos a los que el encargado podrá acceder a aquellos que sean necesarios para realizar su labor.

Como se vio, al abordar la delimitación entre responsable y encargado, la finalidad del tratamiento es esencial para determinar si estamos ante un responsable o un encargado del tratamiento. En el momento en el que el encargado decida tratar los datos, a los que tiene acceso, para otra finalidad distinta a la indicada por el responsable para prestarle el servicio, se considerará que es responsable. Esto se entronca con la legitimación, ya que el responsable, cuando decide realizar un tratamiento, debe apoyarse en una base jurídica. En consecuencia, cuando el responsable decide que, para realizar ese tratamiento le va a dar acceso a un prestador de servicios, la legitimación se extiende al tratamiento que realiza ese prestador, siempre que se mantengan la finalidad y las garantías[1030].

Otro requisito para que se aplique esta regulación es que el encargado debe prestar un servicio al responsable[1031]. La prestación de servicios es por naturaleza onerosa, por lo

[1029] J. RUBÍ NAVARRETE, "El encargado del tratamiento", A. PALOMAR OLMEDA, P. GONZÁLEZ ESPEJO (dirs.); C. ÁLVAREZ RIGAUDIAS (Coord.), VVAA, *Comentario al Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal: (aprobado por RD 1720/2007, de 21 de diciembre), op. cit.*, pág. 221.

[1030] Como indicó la Audiencia Nacional: "En suma, existe encargo de tratamiento cuando la transmisión o cesión de datos está amparada en la prestación de un servicio que el responsable del tratamiento recibe de una empresa externa o ajena a su propia organización, y que le ayuda en el cumplimiento de la finalidad del tratamiento de datos consentida por el afectado." SAN de 16 de julio de 2009 (Sala de lo contencioso-administrativo) (ROJ: SAN 3789/2009), FJ 6.

[1031] Así el Tribunal Supremo estimó que no existía esta prestación de servicios en un asunto, en el que una inmobiliaria suscribió un contrato con la entidad bancaria BBVA, mediante el que esta última se comprometía a ofrecer a los clientes de la primera una oferta de financiación por la compra de inmuebles. Para ello, la inmobiliaria entregaba un listado de sus clientes al BBVA que les enviaba estas ofertas. La inmobiliaria alegaba que el contrato debía encuadrarse en el artículo 12 LOPD porque el BBVA actuaba como encargado del tratamiento, al llevar a cabo un tratamiento encargado por la inmobiliaria. Sin embargo el Tribunal Supremo consideró que el contrato era de prestación de servicios recíprocos, en interés de ambos contratantes y no una externalización de servicios. STS de 29 de junio de 2010 (Sala 3ª) (ROJ: STS 3674/2010), FJ 2.

que se suscitó la cuestión de si sólo podía ser encargado del tratamiento aquel a quien se le contrate un servicio y se le pague un precio por esta prestación. Con la aprobación del RLOPD se resolvió este aspecto, al establecerse que la prestación de servicios puede ser de carácter remunerado o no, y además se añade que podrá ser temporal o indefinida (art. 20.1 RLOPD)[1032].

Es obligatorio que responsable y encargado suscriban un contrato (art.12.2 LOPD). Esta disposición sigue la regulación del artículo 17.3 Directiva 95/46/CE, aunque se pueden apreciar algunas diferencias. La LOPD exige que la realización del tratamiento de datos por cuenta de terceros se regule en un contrato, que debe constar por escrito o en alguna otra forma, que permita acreditar su celebración y contenido[1033]. La Directiva 95/46/CE, sin embargo, lo que indica es que la regulación deberá incluirse en un contrato u otro acto jurídico, que vincule al encargado del tratamiento con el responsable del tratamiento. Por tanto, la LOPD se centra en la forma del contrato y la Directiva 95/46/CE se refiere a la naturaleza del instrumento que vincula a ambas partes, de forma que amplía la misma a cualquier acto jurídico que tenga esa capacidad.

El hecho de no cumplir con este deber formal de suscribir un contrato se sanciona como una infracción leve, gracias al cambio en el marco sancionador de la LOPD, ya que antes se consideraba infracción grave[1034]. Esta tipificación se podrá aplicar en los

[1032] Esta cuestión se suscitaba especialmente en grupos de empresas, donde una de ellas centralizaba la gestión administrativa y, por tanto, trataba datos por cuenta del resto de empresas del grupo. Sin embargo, la ACPD en una recomendación principalmente dirigida al sector público, deja claro que el encargo puede ser a título gratuito o remunerado y que la contraprestación puede ser a cargo del responsable o mediante la percepción de tasas, precios públicos u otros ingresos satisfechos por las personas usuarias del servicio. Recomendación 1/2010 de la Agència Catalana de Protecció de Dades, sobre el encargado de tratamiento en la prestación de servicios por cuenta de entidades del sector público de Cataluña, apdo. 4.5.

[1033] No puede aplicarse el principio de libertad de forma y dar por válido un pacto verbal, ya que el objetivo de la norma es "garantizar que el acceso de terceros a los datos de carácter personal únicamente se produzca en los casos y con las limitaciones legalmente establecidas, plasmándose las condiciones, la finalidad y el alcance de la cesión, de forma que resulte controlable en su desarrollo y cumplimiento." STS de 4 de mayo de 2009 (Sala 3ª) (ROJ: STS 2651/2009), FJ 2 y SAN de 15 de noviembre de 2002 (Sala de lo contencioso-administrativo) (ROJ: SAN 6324/2002), FJ 4. No obstante, hay que decir que la AEPD ha admitido que no existiera contrato en un supuesto del sector público, en el que la Gerencia Informática de la Seguridad Social prestaba servicios informáticos a otros órganos del Ministerio, Entidades Gestoras y Servicios Comunes de la Seguridad Social. La AEPD entendió que el contrato se podía sustituir por el real decreto que establecía las funciones y competencias de la gerencia y que incluía los aspectos necesarios según el artículo 12.2 LOPD, Informe 333/2012 AEPD.

[1034] Anteriormente a este cambio de marco sancionador que tuvo lugar en el año 2011 (ver Capítulo VII) esta infracción de los deberes formales establecidos por el artículo 12.2 LOPD se incluía en el antiguo artículo 44.3.d) LOPD, que tipificaba como infracción grave "tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de

supuestos en los que se determine que estamos ante un encargado del tratamiento y que no se ha cumplido con este deber formal.

La LOPD amplía, respecto a lo establecido en la Directiva 95/46/CE, el contenido preceptivo que debe introducirse en el contrato, de forma que debe indicar:

> "que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 LOPD que el encargado del tratamiento está obligado a implementar" (art. 12.2 LOPD)[1035].

En lo relativo a las instrucciones del responsable, la Directiva 95/46/CE se refiere al comportamiento general que debe tener el encargado: debe actuar de acuerdo con estas instrucciones. La LOPD se refiere al tratamiento de datos: el encargado debe tratar los datos conforme a las instrucciones del responsable. También es diferente la redacción sobre el cumplimiento de las medidas de seguridad, ya que mientras la Directiva 95/46/CE se centra en que debe especificarse que el cumplimiento de las mismas también incumbe al encargado, en la LOPD a lo que se obliga es a indicar las concretas medidas de seguridad que debe aplicar el encargado[1036].

En la LOPD se establecen unos aspectos que se añaden a los que contemplaba la Directiva 95/46/CE y que son los que se han subrayado en el texto del precepto. Se deja claro que los datos no se pueden utilizar para fines distintos al objeto del contrato y que los datos no se comunicarán a terceros, ni siquiera para su conservación. Esta última previsión originó muchos problemas en la práctica, ya que vetaba, de forma absoluta, la posibilidad de que el encargado del tratamiento subcontratara, total o parcialmente, el

---

desarrollo, cuando no constituya infracción muy grave". Esta infracción había sido muy criticada por su amplitud y por eso se modificó, de forma que en el nuevo marco sancionador, se especificó que el tratamiento debía conculcar los principios y garantías del artículo 4 LOPD (actual art. 44.3.c) LOPD). Se puede citar, como ejemplo de resolución de la AEPD que anteriormente al cambio del marco sancionador, aplicaba el tipo del antiguo artículo 44.3.d) LOPD y que esgrimía la jurisprudencia de la Audiencia Nacional en su defensa, la Resolución R/02340/2009 del Procedimiento nº PS/00381/2009 de 20 de noviembre de 2009.

[1035] El subrayado es de la autora. La Directiva 95/46/CE exige que ese acto jurídico incluya el siguiente contenido: "que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento; que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado incumben también a éste" (art. 17.3 Directiva 95/46/CE).

[1036] Esto implica el desarrollo de todas las medidas que debe aplicar el encargado para cumplir con lo establecido en el Título VIII RLOPD, si bien hay que decir que, en muchas ocasiones, en la práctica se suele reproducir la fórmula del principio de seguridad (art. 9 LOPD) y el nivel de medidas que el encargado debe aplicar.

objeto del contrato. La subcontratación es un fenómeno generalizado en nuestros días y este precepto lo que hacía era prohibirlo, con los subsiguientes perjuicios para la competitividad de las empresas españolas. Por ello, la AEPD realizó una interpretación que permitía la subcontratación si se cumplían unos requisitos[1037]. Esta interpretación se incorporó en el RLOPD y se abordará en el siguiente apartado.

Adicionalmente, otro aspecto que deberá incluirse en el contrato, suscrito entre el responsable y el encargado, es si se ha delegado por parte del responsable la llevanza de su documento de seguridad en el encargado del tratamiento (art. 88.6 RLOPD).

A diferencia de la Directiva 95/46/CE, la LOPD estipula que, cuando se haya cumplido la prestación contractual, el encargado del tratamiento deberá destruir o devolver al responsable los datos de carácter personal, al igual que cualquier soporte o documentos en que conste algún dato objeto del tratamiento (art. 12.3 LOPD). De nuevo, esta previsión ponía en un aprieto al encargado que, según la misma, no podía conservar ningún dato de carácter personal, que hubiera tratado, en el marco de la relación contractual que le unía con el responsable.

¿Qué sucedería entonces si el responsable decidía interponer una demanda contra el encargado del tratamiento por algún problema derivado de la prestación contractual? El responsable podría esperar a la finalización de esta prestación, de forma que el encargado no dispondría de los datos de carácter personal que podría precisar, como evidencias para probar su buen hacer en el desarrollo de ese contrato. Por tanto, como consecuencia tendríamos la vulneración del derecho de defensa del encargado del tratamiento establecida en el artículo 24 CE[1038].

Tampoco parecía lógico que tuviera estas consecuencias la finalización del contrato para el encargado del tratamiento, cuando la LOPD establece para los tratamientos, que lleve a cabo un responsable del tratamiento, la obligación de bloqueo de

[1037] Recomendaciones referentes al plan de inspección de oficio a las empresas participantes en la elaboración de los censos de población y viviendas del año 2001 de 17 de julio de 2003.
[1038] J. RUBÍ NAVARRETE, "El encargado del tratamiento", A. PALOMAR OLMEDA, P. GONZÁLEZ ESPEJO (dirs.); C. ÁLVAREZ RIGAUDIAS (Coord.), VVAA, *Comentario al Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal: (aprobado por RD 1720/2007, de 21 de diciembre), op. cit.*, pág. 243.

los datos personales, precisamente para poder dirimir responsabilidades que puedan nacer del tratamiento.

El RLOPD se dedica a esta cuestión y si bien, vuelve a repetir la obligación del encargado de destruir o devolver al responsable los datos, al finalizar la prestación contractual, se añade que el encargado debe conservar los datos, si se pudieran derivar responsabilidades de su relación con el responsable (art. 22 RLOPD). Esta conservación deberá realizarse, de forma que los datos estén debidamente bloqueados[1039].

También en el RLOPD se añade que la devolución de los datos al responsable se podrá realizar, no directamente al responsable, sino al nuevo encargado del tratamiento que pudiera haber designado este responsable[1040]. Asimismo, el encargado no podrá destruir los datos, cuando exista una previsión legal que exija su conservación. En este caso, se obliga a la devolución de estos datos, de forma que se garantice al responsable la conservación[1041].

Otro aspecto que se encuentra en la Directiva 95/46/CE y que no se había recogido en la LOPD es la obligación del responsable del tratamiento a elegir un encargado del tratamiento, que reúna garantías suficientes respecto al cumplimiento de las medidas de seguridad que debe adoptar y el seguimiento de que el encargado cumple estas medidas (art. 17.2 Directiva 95/46/CE).

De nuevo, se corrigió este defecto de la transposición y se introdujo este precepto en el artículo 20.2 RLOPD, de forma que obliga al responsable a velar porque el encargado del tratamiento reúna las garantías, para el cumplimiento de lo dispuesto en el RLOPD. Por tanto, se amplía el alcance de esta obligación, ya que no se limitará a las medidas de seguridad, sino a toda la regulación sobre el encargo del tratamiento. No

[1039] Lo que, de acuerdo con el artículo 16.3 LOPD y la definición de cancelación del artículo 5.1.b RLOPD, implica que los datos se conservarán únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

[1040] De esta forma, se regula lo que se denomina la portabilidad de los datos, que pretende agilizar el cambio de encargado del tratamiento.

[1041] Al redactarse esta obligación de forma neutra sin establecer una asignación expresa al encargado de la misma, cabe plantearse si podría responsabilizarse al encargado del incumplimiento. En este sentido, cabe destacar la debilidad del cuadro sancionador de la LOPD, en lo que respecta a la figura del encargado del tratamiento, ya que pocas son las infracciones que podrán ajustarse al mismo.

obstante, si bien se amplía en ese sentido, por otro lado se restringe, ya que no se especifica que el responsable debe asegurarse del cumplimiento de las medidas durante la prestación del servicio. De todas formas, las autoridades de control entienden que debe existir esta obligación *in vigilando*, además de la obligación *in eligendo* inicial[1042].

4.2.3. El régimen de la subcontratación

Tal como se ha indicado, una de las problemáticas que planteó el artículo 12 LOPD fue la imposibilidad de que el encargado del tratamiento pudiera subcontratar a terceros. Esto se resolvió mediante la regulación del artículo 21 RLOPD. De esta forma, se establece en este precepto la regla general de prohibición de subcontratación por parte del encargado del tratamiento y dos vías excepcionales para realizar la misma. Al ser excepciones deberán interpretarse de forma restrictiva.

Según el precepto, la primera vía para poder subcontratar consistiría en que el encargado del tratamiento solicite autorización al responsable. Sin embargo, lo que se establece es que la subcontratación deberá realizarse en nombre y por cuenta del responsable (art. 21.1 RLOPD)[1043]. Por tanto, hay que entender que estamos ante un supuesto de representación o apoderamiento, de forma que el responsable contrata

[1042] La AEPD entiende que el artículo 20.2 RLOPD introduce un poder de supervisión del responsable sobre el encargado, que se traduce en que podrá realizar controles durante el período de vigencia del contrato para verificar el cumplimiento de las medidas de seguridad establecidas. Asimismo, la AEPD indica que el cliente de servicios de *cloud computing* debe poder comprobar las medidas de seguridad del proveedor y puede acordarse que un tercero independiente audite la seguridad. Informe 457/2008 la AEPD y Guía para clientes que contraten servicios de *Cloud Computing*, Agencia Española de Protección de Datos, *op. cit.* págs. 16 a 17. La ACPD recomienda que, en el ámbito del sector público, se cumpla con la obligación de velar porque el encargado reuna las garantías previstas en la normativa, a través de la evaluación de la solvencia técnica, por ejemplo mediante la acreditación con algún certificado, sello de calidad o documentos equivalentes reconocidos en materia de protección de datos o de seguridad de la información. Respecto a que el responsable verifique que el encargado cumpla con la normativa, durante el encargo, la ACPD recomienda que se someta al encargado a auditorías que podrán realizar o el responsable o terceros contratados por el responsable, independientemente del nivel de medidas de seguridad aplicable. Recomendación 1/2010 de la Agència Catalana de Protecció de Dades, sobre el encargado de tratamiento en la prestación de servicios por cuenta de entidades del sector público de Cataluña, apdos 9.1 y 31.

[1043] Esto exigirá, por lo tanto, el otorgamiento por parte del responsable de un poder específico al encargado para realizar esta contratación en su nombre y por su cuenta. En este sentido, el artículo 247 Código de Comercio establece que "si el comisionista contratare en nombre del comitente, deberá manifestarlo y si el contrato fuere por escrito, expresarlo en el mismo en la antefirma, declarando el nombre, apellido y domicilio de dicho comitente. (…) el contrato y las acciones del mismo producirán su efecto entre el comitente y la persona o personas que contrataren con el comisionista; pero quedará éste obligado con las personas con quienes contraté, mientras no pruebe la comisión, si el comitente la negare, sin perjuicio de la obligación y acciones respectivas entre el comitente y el comisionista."

directamente con el subencargado, aunque sea el encargado quien lo haga en su nombre[1044].

La segunda vía para que el encargado pueda realizar la subcontratación es que se especifiquen, en el contrato suscrito entre el responsable y el encargado, los servicios que puedan ser objeto de subcontratación y, si fuera posible, la empresa con la que se van a subcontratar. En caso de que no fuera posible identificar a esta empresa, el responsable deberá comunicarlo al responsable, antes de subcontratar[1045].

Para poder optar por esta segunda vía, el tratamiento de datos que realice el subcontratista debe ajustarse a las instrucciones del responsable del fichero, de forma que se asegura que el responsable no pierda el control sobre los datos. Por último, el encargado y el subcontratista deben formalizar un contrato, que cumpla los mismos requisitos legales enunciados para el contrato entre encargado y responsable. El subcontratista debe considerarse encargado del tratamiento y, por tanto, se le aplicará todo lo establecido en la normativa para esta figura[1046]. Hay que entender que, pese a que el RLOPD no lo indique expresamente, el responsable debe disponer de poder de decisión respecto a los servicios subcontratados y también respecto a la entidad subcontratada[1047].

[1044] Así lo indican J.L. PIÑAR MAÑAS, "Posibilidad de subcontratación de los servicios", J. ZABÍA DE LA MATA (Coord.), VVAA, *Protección de datos: comentarios al Reglamento*, Lex Nova, Valladolid, 2008, págs. 240 a 241 y S. FARRÉ TOUS, "El encargado del tratamiento en el ámbito de las administraciones públicas", A. TRONCOSO REIGADA, A. (Dir.). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, págs. 1.111 a 1.112.

[1045] En entornos complejos en los que puede ser posible la subcontratación de una múltitud de proveedores por parte del encargado o incluso que pueda haber un gran movimiento de cambio en los mismos, como puede ser en servicios de *cloud computing*, la AEPD ha estimado adecuado que se pueda informar sobre las empresas, por ejemplo, mediante la publicación del listado en un sitio web. Guía para clientes que contraten servicios de *Cloud Computing*, Agencia Española de Protección de Datos, *op. cit.* pág. 14.

[1046] Como indica PIÑAR MAÑAS, en esta segunda vía, es necesario aclarar que el subcontratista será considerado encargado del tratamiento, ya que así, podrá ser sujeto responsable a efectos de la LOPD. En la primera vía no es necesario realizar esta aclaración porque al ser un supuesto de representación, el responsable contrata directamente con el subencargado, de manera que no existe subcontratación y este subencargado, en realidad, es un encargado. J.L. PIÑAR MAÑAS, "Posibilidad de subcontratación de los servicios", J. ZABÍA DE LA MATA (Coord.), VVAA, *Protección de datos: comentarios al Reglamento*, Lex Nova, Valladolid, 2008, pág. 245.

[1047] Como indica RUBÍ NAVARRETE se puede hallar un argumento para afirmar este control en el artículo 21.2.b) RLOPD, que establece que el tratamiento del subcontratista debe ajustarse a las instrucciones del responsable, lo que unido a su deber de diligencia debe conducir a esta capacidad de decisión. Como indica el autor, a la necesidad de que el encargado comunicara la identidad del subcontratado al responsable se opusieron los empresarios, durante el proceso de aprobación del RLOPD (en concreto a través de la Confederación Española de Organizaciones empresariales o CEOE), ya que el hecho de desvelar estas subcontrataciones podía suponer la contratación directa entre responsable y subcontratado. J. RUBÍ NAVARRETE, "El encargado del tratamiento", A. PALOMAR OLMEDA, P. GONZÁLEZ ESPEJO (dirs.); C. ÁLVAREZ RIGAUDIAS (Coord.), VVAA, *Comentario al Reglamento de desarrollo de la Ley*

Si fuera durante la prestación del servicio cuando se planteara la necesidad de subcontratar el servicio y no se hubiera previsto esta circunstancia en el contrato, se exige que el encargado cumpla con lo establecido respecto a la segunda vía (art. 21.3 RLOPD).

Por último, hay que recordar que la subcontratación debe referirse a un tratamiento que le hubiera encomendado el responsable del tratamiento (art. 21.1 RLOPD). En consecuencia, el encargado podrá contratar servicios, en calidad de responsable, que impliquen acceso a datos de sus propios ficheros o tratamientos. Pero ¿qué sucede con aquellos servicios que no se dediquen de forma específica al tratamiento encomendado, sino que sean contratados por el encargado y alcancen a todos sus tratamientos como los servicios de tipo informático?

Ya se analizó que el encargado podrá decidir sobre los medios no esenciales del tratamiento lo que afectaba, inicialmente a la elección de medios técnicos (no en lo que se refiere a las medidas de seguridad). Sin embargo, de lo que trata la subcontratación es de la decisión sobre quién podrá acceder a los datos, aspecto que debe incluirse entre los medios esenciales del tratamiento. Por tanto, pese a que el servicio no se dedique, de forma específica a realizar el tratamiento encomendado deberá someterse a la regulación de la subcontratación[1048].

4.3. Las transferencias de datos a países terceros

Las transferencias de datos a países terceros se hallan reguladas en los artículos 33 y 34 LOPD, desarrollados por los artículos 65ss RLOPD y que se completa con los artículos 137ss RLOPD que regulan los procedimientos que tramita la AEPD relacionados con estas transferencias: el de autorización y el de suspensión temporal de las mismas.

Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal: (aprobado por RD 1720/2007, de 21 de diciembre). op. cit., págs. 234 a 235.

[1048] RUBÍ NAVARRETE, cuando indica que no estima necesario que deban incluirse en el contrato entre responsable y encargado instrucciones específicas del responsable para el subcontratista, hace mención a la variedad de servicios que pueden subcontratarse como los horizontales o coadyuvantes a la propia actividad del encargado, por ejemplo, para la asistencia informática, o verticales, como los que suponen que un tercero realice materialmente tratamientos de datos que el propio encargado asumió para prestar el servicio. En consecuencia, estima este autor, que ambos tipos de servicios están sometidos a la regulación de la subcontratación. *Ibídem*, pág. 236.

Es importante tener en cuenta que se trata de una regulación especial que, por tanto, se añade a la regulación general. Es decir, si un responsable debe transmitir datos personales a un país extranjero deberá cumplir con lo establecido en la normativa, al igual que debe hacerlo en una transmisión de datos nacional. Por tanto, la transmisión de datos deberá calificarse como cesión o como encargo del tratamiento y cumplir todo lo previsto para estos supuestos, así como el resto de los otros principios aplicables de la normativa. De forma adicional, el responsable deberá ajustarse a lo indicado en esta regulación de las transferencias internacionales.

4.3.1. Exportador e importador ¿dos nuevos sujetos?

El RLOPD introdujo dos nuevos conceptos relacionados con el régimen de las transferencias internacionales que no aparecían en la LOPD: el exportador y el importador de datos personales.

> "Exportador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero." (art. 5.1.j) RLOPD)
> "Importador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero." (art. 5.1.ñ) RLOPD)

¿Estamos ante nuevos sujetos obligados diferenciados del responsable y del encargado? Como vemos, en la definición de importador queda claro que no nos referimos a un nuevo sujeto, sino que se asigna un nuevo papel a los sujetos ya definidos (responsable, encargado o tercero). El concepto de exportador, sin embargo, se desvincula de los sujetos ya definidos y, aparentemente, se trata de un nuevo sujeto que no tiene porque ser ni responsable ni encargado.

Los conceptos de exportador e importador se introdujeron en las cláusulas tipo que aprobó la Comisión Europea para facilitar la aportación de garantías en procedimientos de

solicitud de autorización y que veremos más adelante. Sin embargo, en estos textos el concepto de exportador se refiere claramente al responsable del tratamiento[1049].

El legislador aprovechó la neutralidad con la que se había configurado la regulación de las transferencias internacionales en la LOPD, en la que no hay asignación expresa de la obligación al responsable e introdujo este concepto de exportador, sin definir al sujeto al que debía asignarse el papel.

Cuando se aprobó el RLOPD, la AEPD, al igual que el resto de las autoridades mediante el GA29, habían iniciado un proceso de flexibilización en el régimen de autorización de las transferencias, mediante la creación de nuevos mecanismos que facilitaran la solicitud a las empresas. Como se verá, no sólo se quiso facilitar el proceso a los responsables, sino también a los encargados europeos que quisieran subcontratar a prestadores de servicios que se hallaran ubicados fuera del EEE.

La AEPD aprovechó la neutralidad, establecida en la LOPD, para entender que el exportador podía ser también un encargado del tratamiento. De esta forma, el encargado podía iniciar el trámite de autorización y facilitar así a sus clientes el procedimiento. En conclusión, la definición del RLOPD responde a una finalidad puramente funcional[1050].

[1049] En todas las cláusulas tipo aprobadas por la Comisión incluye la definición de "exportador de datos" que "se entenderá el responsable del tratamiento que transfiera los datos personales" (arts. 3.d) Decisión 2001/497/CE, apdo. b) definiciones en Anexo a la Decisión 2004/915/CE, 3.c) Decisión de la Comisión C(2010)593 final). El "importador de datos" depende de si se define en las cláusulas que se aplican a la transferencia de datos entre dos responsables o si es en las cláusulas que se aplican a una transferencia entre un responsable y un encargado del tratamiento. En el primer caso el importador de datos "se entenderá el responsable del tratamiento que acepte recibir datos personales procedentes del exportador de datos para su posterior tratamiento de conformidad con los términos de las presentes cláusulas y que no esté sujeto al sistema de un tercer país por el que se garantice una protección adecuada" (apdo. c) definiciones en Anexo a la Decisión 2004/915/CE). En el segundo caso el importador de datos es "el encargado del tratamiento establecido en un tercer país que convenga en recibir del exportador datos personales para su posterior tratamiento en nombre de éste, de conformidad con sus instrucciones y los términos de la presente Decisión, y que no esté sujeto al sistema de un tercer país que garantice la protección adecuada en el sentido del artículo 25, apartado 1, de la Directiva 95/46/CE" (3.d) Decisión de la Comisión C(2010)593 final). La AEPD señalaba esta rigidez en Informe 0582/2004.

[1050] Señala esta finalidad puramente técnica de los conceptos de importador y exportador C. ÁLVAREZ RIGAUDIAS, "Las transferencias internacionales de datos personales", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, *op. cit.*, pág. 1.803.

4.3.2. La prohibición general de realizar transferencias y sus excepciones

La LOPD establece una prohibición general de realizar transferencias de datos de carácter personal con destino a países que no proporcionan un nivel de protección equiparable al que presta la LOPD, salvo que, además de cumplir esta, se obtenga la autorización del Director de la AEPD (art. 33.1 LOPD)[1051]. No obstante, se establecen una serie de situaciones excepcionales a esta regla general, en las que podrá realizarse la transferencia a estos países sin nivel equiparable, sin necesidad de obtener la autorización (art. 34 LOPD). Estas excepciones son:

> "a) cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España; b) cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional; c) cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios; d) cuando se refiera a transferencias dinerarias conforme a su legislación específica; e) cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista; f) cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado; g) cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero; h) cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias; i) cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo; k) cuando la transferencia tenga como destino un Estado miembro de la UE, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado." (art. 34 LOPD)

Hay algunas de estas excepciones que no se contemplan en la Directiva 95/46/CE[1052]. Eran supuestos heredados de la LORTAD que se añadieron a los que fueron origen de la transposición[1053]. Los Estados miembros tenían cierto margen de maniobra, ya que la Directiva 95/46/CE les permitía establecer casos particulares en los que no permitieran las transferencias, aunque se pudieran aplicar las excepciones (art. 26.1

[1051] En la exposición de esta regla se observa que se hace referencia al nivel de protección "equiparable", cuando la Directiva 95/46/CE indica "adecuado". El término equiparable provenía de la LORTAD. No obstante el artículo 33.2 LOPD sí alude al carácter adecuado del nivel de protección.

[1052] Serían los apartados a), b) y d) del artículo 34 LOPD.

[1053] El artículo 33 LORTAD contemplaba estas excepciones y añadía otra que se refería a cuando la transferencia tuviera por objeto el intercambio de datos de carácter médico entre facultativos o instituciones sanitarias y así lo exigiera el tratamiento del afectado, o la investigación epidemiológica de enfermedades o brotes epidémicos. Este supuesto se subsumió en el apartado c) del artículo 34 LOPD.

Directiva 95/46/CE). Sin embargo, el listado de excepciones es exhaustivo y ha sido uno de los aspectos que la Comisión Europea ha resaltado en los que hay una falta de armonización, que tiene consecuencias negativas en el mercado interior[1054].

Otra diferencia que destacó la Comisión de la LOPD respecto a la Directiva 95/46/CE fue la del supuesto referente a cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público (art. 34.h) LOPD)[1055]. En la Directiva 95/46/CE lo que se establece es que la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante (art. 26.1.d) Directiva 95/46/CE). La Directiva 95/46/CE, además de no contemplar el ejemplo que introduce la LOPD de la transferencia a una administración fiscal o aduanera, incluye el adjetivo "importante", lo que hace que el supuesto establecido en la normativa española sea más laxo que el de la Directiva 95/46/CE.

La salvaguardia del interés vital del interesado, que se incluye en la Directiva 95/46/CE se ha sustituido en la LOPD por el que permite la transferencia cuando sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios (art. 34.c) LOPD), que no puede considerarse totalmente coincidente.

Por último, entre las excepciones, llama la atención la última relativa a una transferencia, que tenga como destino un Estado miembro de la UE o un Estado respecto del cual la Comisión Europea haya declarado que garantiza un nivel de protección adecuado (art. 34.k) LOPD). Sorprende que se establezca, como un supuesto de excepción, el hecho de transmitir los datos a un Estado miembro de la UE. La Directiva 95/46/CE, al incluir una regulación sobre transferencias de datos a países terceros, se refiere a países externos a la UE. El objetivo de la Directiva 95/46/CE es asegurar la libre

[1054] En el primer informe sobre la transposición de la Directiva 95/46/CE, la Comisión Europea llamaba la atención sobre la falta de uniformidad en el listado de excepciones respecto al que indicaba que no había margen de maniobra posible. *Report from the Commission, First report on the implementation of the Data Protection Directive 95/46/EC, COM(2003) 265 final, Brussels, 15.5.2003*, pág. 11. Entre los países que no habían respetado el listado, la Comisión señalaba España, por incluir supuestos que no figuraban en la lista. *Analysis and impact study on the implementation of Directive EC 95/46 in Member States, Annex to "First report on the implementation of the Data Protection Directive (95/46/EC)", COM(2003) 265 final, Brussels, 15.5.2003,* pág. 33.

[1055] *Analysis and impact study on the implementation of Directive EC 95/46 in Member States, Annex to "First report on the implementation of the Data Protection Directive (95/46/EC)", COM(2003) 265 final, Brussels, 15.5.2003,* pág. 33.

circulación de los datos en el territorio europeo y con la regulación de las transferencias se persigue asegurar un régimen armonizado que, al mismo tiempo que protege los derechos de los ciudadanos europeos, evite que exista una legislación nacional más favorable que otra a las transferencias, que pueda favorecer el *forum shopping*.

De nuevo, este "fallo" se repara en el RLOPD, de forma que se define lo que se considera "transferencia internacional de datos: tratamiento de datos que supone una transmisión de los mismos fuera del territorio del EEE, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero, establecido en territorio español" (art. 5.1.s) RLOPD). Por tanto, deja claro el RLOPD que no sería transferencia internacional de datos la que se realice a un país del EEE.

Esto se completa cuando en el RLOPD se indican los casos en los que no se precisa de autorización del Director de la AEPD: cuando el Estado de destino ofrezca un nivel adecuado y cuando la transferencia se encuentre en uno de los supuestos contemplados en los apartados a) a j) del artículo 34 LOPD (art. 66.2 RLOPD). Por tanto, se obvia el apartado k) del artículo 34 LOPD. El nivel adecuado lo puede estimar el Director de la AEPD, mediante resolución que se publicará en el "Boletín Oficial del Estado" (art. 67 RLOPD). También se reconoce la validez de las decisiones sobre el nivel adecuado que adopte la Comisión Europea (art. 68 RLOPD).

Por último, hay que indicar que, aunque no sea precisa la autorización para realizar la transferencia, ésta debe ser notificada para su inscripción en el Registro General de Protección de Datos (art. 66.3 RLOPD).

Para el GA29 las excepciones no deberían ser la primera opción a la que debería recurrir el responsable, en caso de tener que realizar una transferencia de datos a un país sin nivel adecuado de protección[1056]. Pese a que estos supuestos se han previsto en casos en los que se estima que no hay un elevado riesgo para los derechos, las autoridades han

[1056] Documento de trabajo del Grupo del Artículo 29 relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE, *op. cit.*, pág 11.

manifestado que tiene más garantías la vía de solicitud de autorización[1057]. Por tanto, para transferencias masivas o estructurales, se recomienda no optar por las excepciones que deben utilizarse en casos puntuales[1058].

4.3.3. La autorización para realizar transferencias

Fuera de los casos indicados, en los que se permite la transferencia a países que no cuentan con el nivel adecuado de protección, será necesario solicitar autorización del Director de la AEPD. Esta autorización se otorgará al responsable si este aporta un contrato, en el que consten las garantías de respeto de la protección de la vida privada de los afectados y de sus derechos y libertades fundamentales (arts. 33.1 LOPD y 70 RLOPD)[1059]. Además, se incorpora en el RLOPD un reconocimiento expreso a la validez de las cláusulas tipo aprobadas por la Comisión Europea que podrán utilizarse para obtener la autorización (art. 70.2 RLOPD)[1060].

Asimismo, el RLOPD incluye un instrumento que no se halla en la regulación de la Directiva 95/46/CE, sino que ha sido elaborado por el GA29: las reglas corporativas vinculantes (*Binding Corporate Rules* o BCR)[1061]. Estas reglas, que en el RLOPD se denominan normas o reglas internas, pretenden facilitar el otorgamiento de autorizaciones para la realización de transferencias internacionales, en el marco de grupos multinacionales de empresas (art. 70.4 RLOPD). El RLOPD dispone que estas normas

[1057] El GA29 recomienda que las excepciones se apliquen en los casos en que resulte inadecuado, o hasta imposible, que la transferencia se realice por la vía de la obtención de autorización. Es decir, que considera que si la empresa tiene los medios para adoptar mecanismos de protección como las cláusulas contractuales o las normas corporativas vinculantes, debería hacerlo, antes de optar por las excepciones. *Ibídem.*

[1058] Aunque el GA29 reconoce que, en algunos casos, este tipo de transferencias masivas o reiterativas podrá llevarse a cabo sobre la base de las excepciones si los riesgos para los interesados fueran mínimos, como en el caso de las transferencias de dinero que se realizan a diario y de forma masiva. *Ibídem.*

[1059] Llama la atención esta referencia al derecho a la vida privada y a otros derechos y libertades fundamentales que se debe al hecho de realizar una reproducción del contenido del artículo 26.2 Directiva 95/46/CE que incluye esta referencia, puesto que en la época en la que se aprobó la directiva no existía un reconocimiento del derecho de protección de datos como derecho autónomo, reconocimiento que, como ya se ha abordado en este trabajo, existe actualmente en el artículo 8 Carta UE.

[1060] Se mencionan incluso las Decisiones de la Comisión Europea 2001/497/CE, de 15 de Junio de 2001, 2002/16/CE, de 27 de diciembre de 2001, y 2004/915/CE, de 27 de diciembre de 2004. Sin embargo, este listado ya ha quedado desactualizado, ya que la Decisión 2002/16/CE, de 27 de diciembre de 2001 fue derogada por la Decisión de la Comisión 2010/87/UE relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 5 de febrero de 2010.

[1061] Ver Capítulo V.

deban tener carácter vinculante para las empresas del grupo y ser exigibles conforme al ordenamiento español.

Ya indicábamos que el legislador había aprovechado la neutralidad de la asignación de la obligación en materia de transferencias internacionales, para incluir los conceptos de exportador e importador, con la intención de que el exportador pudiera ser también un encargado del tratamiento. El RLOPD, en línea con esta neutralidad, respecto a las BCR, alude a que la autorización se podrá otorgar "en el seno de grupos multinacionales". De esta forma, también se podrá incluir en esta disposición la utilización por grupos multinacionales de las reglas corporativas vinculantes para encargados del tratamiento (*Binding Corporate Rules for Processors* o BPR), que como vimos, están destinadas a facilitar las autorizaciones para encargados del tratamiento[1062].

Hay que resaltar el papel impulsor de la AEPD, en la flexibilización de los procesos de autorización de transferencias internacionales. En este sentido, la AEPD ha permitido que los encargados del tratamiento españoles puedan solicitar autorizaciones, con el objetivo de que puedan subcontratar a terceros prestadores que se hallan en países sin nivel adecuado de protección[1063]. Si se sigue el procedimiento normal, serían los clientes de estos encargados, que se consideran responsables del tratamiento, quienes tendrían que solicitar la autorización, con el fin de que los encargados pudieran subcontratar sus servicios. Esto supone una importante traba comercial para estos encargados.

Con esta nueva modalidad, el encargado es quien tiene la iniciativa en el proceso de autorización. Es este quien solicita la autorización y para obtenerla debe presentar el contrato que ha suscrito con el sub-encargado del tratamiento. Este contrato obedece al modelo aprobado por la AEPD, en virtud de las cláusulas tipo de la Comisión Europea y que también respeta la legislación española[1064]. Asimismo, el encargado solicitante debe aportar un contrato tipo que suscribirá con sus clientes, responsables.

[1062] Ver Capítulo V.
[1063] La primera de estas resoluciones fue la Resolución TI/00126/2012 de 16 de octubre de 2012.
[1064] El contrato suscrito entre el encargado exportador y el subencargado importador deberá cumplir con los requisitos establecidos en la legislación española en lo que se refiere a la subcontratación de servicios (concretamente en el art. 21 RLOPD) y también con lo que establece al respecto la Decisión 2010/87/UE de la Comisión que aprobó las cláusulas tipo para la transferencia de datos a encargados del tratamiento (concretamente en su cláusula 11).

De esta forma, no será necesario que el encargado vuelva a someterse al trámite por cada uno de los clientes que tenga, sino que bastará con que utilice este contrato tipo aprobado por la AEPD. El cliente, por su lado, lo que deberá hacer es notificar que se va a realizar la transferencia, de forma que la AEPD podrá comprobar, mediante la información que el encargado le debe proporcionar que, efectivamente, se trata de uno de los clientes del encargado que se ha sometido al trámite de autorización[1065].

El modelo de cláusulas aprobado por la AEPD, que sirven al encargado, exportador, para elaborar el contrato con el sub-encargado, importador, es el que ha presentado el GA29 a la Comisión Europea para que considere su aprobación[1066].

En línea con este ánimo impulsor, la AEPD ha otorgado una autorización a la compañía *Microsoft*, con el mismo sistema, pero que conlleva unas adaptaciones dirigidas a las especialidades del sector de la computación en la nube (*cloud computing*)[1067]. El GA29, con el que había contactado *Microsoft* antes de seguir el trámite con la AEPD directamente, manifestó su conformidad con este modelo[1068].

Finalmente, no hay que olvidar que, a efectos de solicitar la autorización para realizar la transferencia, es importante que el responsable cumpla con lo establecido en la LOPD y el RLOPD (arts. 33.1 LOPD y 65 RLOPD). De esta forma, la AEPD, para otorgar una autorización se detendrá en el examen del instrumento contractual o las reglas internas que se presenten, para dirimir si cumplen la regulación que se aplique al supuesto concreto en la normativa española.

[1065] El encargado del tratamiento exportador de los datos deberá poner a disposición de la AEPD los contratos suscritos con sus clientes por la prestación de servicios y dispondrá de una lista actualizada de estos responsables y de los ficheros transferidos, que comunicará al Registro General de Protección de Datos.

[1066] Ver Capítulo V.

[1067] Esta nueva especialidad de autorizaciones de transferencias internacionales se presentó en la 5ª Jornada Abierta que celebró la AEPD, en el 2013, y se ha utilizado en la Resolución TI/00032/2014 de 9 de mayo de 2014 que ha servido para autorizar la transferencia internacional de datos originada por la contratación de los servicios de *cloud computing* de Microsoft Corporation, empresa estadounidense (en concreto los servicios *Office 365*, *Microsoft Dynamics CRM online* y *Windows azure)*.

[1068] Carta del GA29, mediante la que estiman que el contrato presentado cumple con lo establecido en la Decisión 2010/87/UE http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf (fecha consulta: 21.8.2015).

La AEPD tiene la capacidad, en virtud del artículo 37.1.f) LOPD[1069], de acordar la suspensión temporal de la transferencia, tanto si la misma es a un Estado que no cuenta con el nivel adecuado de protección, cuando se haya otorgado una autorización (art. 70.3 RLOPD), como si es a un Estado del que se haya declarado el nivel adecuado (art. 69 RLOPD)[1070]. En el primer caso, también se da la posibilidad a la AEPD de denegar la transferencia, lo que debe entenderse que se refiere a que podrá denegar la autorización para realizar la transferencia. No se ha establecido esta posibilidad de suspensión para los casos en que el responsable se acoja a las excepciones del artículo 34 LOPD[1071].

5. DERECHOS O FACULTADES

5.1. La asignación de derechos o facultades

Del mismo modo que se señalaba respecto a la Directiva 95/46/CE, en la legislación española tampoco se asignan de forma expresa derechos al responsable del tratamiento. Sin embargo, se pueden extraer de las obligaciones, establecidas en la LOPD, algunas facultades o derechos para este responsable: el derecho a tratar datos personales, si el responsable cuenta con el consentimiento del titular de los datos o puede acogerse a alguno de los supuestos exceptuados del requisito de consentimiento (art. 6 LOPD), lo que implica que se debe cumplir con las disposiciones establecidas en la LOPD que resulten aplicables al tratamiento concreto de datos; en caso de ser responsables de los sectores específicos regulados en la LOPD, podrán tratar los datos, de acuerdo con lo

[1069] Este artículo permite a la AEPD requerir a los responsables y a los encargados del tratamiento para que adopten las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de la ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros cuando no se ajuste a sus disposiciones

[1070] Esta suspensión se podrá acordar por el Director de la AEPD en virtud de las circunstancias que se indican como, por ejemplo, si es a un Estado con el nivel adecuado, si existen indicios racionales de que se están vulnerando las normas o, en su caso, los principios de protección de datos por la entidad importadora de la transferencia, y que las autoridades competentes en el Estado en que se encuentre el importador no han adoptado o no van a adoptar en el futuro las medidas oportunas para resolver el caso en cuestión, habiendo sido advertidas de la situación por la AEPD. En este caso se podrá suspender la transferencia cuando su continuación pudiera generar un riesgo inminente de grave perjuicio a los afectados.

[1071] Como indica ÁLVAREZ RIGAUDIAS resulta sorprendente aunque señala esta autora la posibilidad de que el artículo 69 RLOPD, al referir su aplicación a los artículos precedentes también incluyera los artículos que están en el Capítulo precedente y que hacen mención a la aplicación de las exepciones. En caso contrario, como indica la autora, lo que le restará a la AEPD es la posibilidad de llevar a cabo la suspensión en función del artículo 37.1.f) LOPD, aunque éste deberá fundarse en la legitimidad de la transferencia por no concurrir las excepciones. C. ÁLVAREZ RIGAUDIAS, "Las transferencias internacionales de datos personales", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, págs. 1.814 a 1.815.

indicado en el sector concreto (arts. 22, 29 a 31 LOPD); tratar o comunicar datos especialmente protegidos en los casos previstos (arts. 7, 8, 11, 22 LOPD); comunicar datos personales si se cumple lo establecido en la normativa (arts. 11, 21, 27 LOPD); contratar servicios que impliquen el acceso a datos personales si se respeta la regulación del encargo del tratamiento (art. 12 LOPD); aplicar las excepciones establecidas para el ejercicio de los derechos de acceso, rectificación, cancelación y el deber de información (arts. 23, 24 LOPD); formular códigos tipo y depositarlos en el Registro General de Protección de Datos (arts. 32 LOPD) y a que los funcionarios inspectores de la AEPD guarden secreto sobre las informaciones que conozcan en el ejercicio de sus funciones (art. 40.2 LOPD).

A continuación se realiza una breve aproximación a lo que se puede considerar el derecho a tratar datos por parte del responsable y a formular códigos tipo y depositarlos en el Registro General de Protección de Datos.

5.2. El derecho a tratar datos

Al igual que se indicaba en referencia a la regulación de la Directiva 95/46/CE, en la legislación española también debe considerarse que el responsable ostenta un derecho o, al menos, una facultad a tratar los datos personales, si lo hace en el respeto de los requisitos que esta normativa dispone. Sin embargo ¿hasta dónde llega este derecho o facultad? Y es que cabe plantear si el régimen establecido en la LOPD exige para poder tratar datos personales contar, de forma previa con una base jurídica legitimadora o si, por el contrario, permitiría una legitimación *a posteriori*.

El artículo 6 LOPD exige para poder tratar datos el consentimiento, salvo que la ley disponga otra cosa, por lo que debe deducirse que será preciso contar siempre con una base jurídica previa para poder tratar datos. Ahora bien, tras la sentencia del TJUE[1072], que estimó la aplicación directa del artículo 7.f) Directiva 95/46/CE, relativo a la legitimación del tratamiento por el interés legítimo del responsable, parece que ha disminuido el control previo de la legitimación. Hay que recordar que, con la regulación anterior a esta sentencia, el supuesto relativo al interés legítimo se limitaba a la

[1072] Sentencia del TJUE de 24 de noviembre de 2011, *ASNEF, FECEMD/Administración del Estado*, C-468/10 y C-469/10, EU:C:2011:777.

utilización, en ese caso, de datos que provenían de fuentes accesibles al público. Estas fuentes están tasadas y no incluyen Internet.

Sin embargo, tras la sentencia mencionada, el responsable puede alegar que posee este interés legítimo para tratar datos, sin tener que circunscribirse a las fuentes accesibles al público. Podrá, por tanto, extraer datos de Internet y utilizarlos con el fin de satisfacer ese interés[1073]. Evidentemente, existe la garantía de la ponderación que debe realizar ese responsable, con el fin de asegurarse de que no prevalezcan los derechos de los interesados, por encima de su interés.

Otra cuestión que se señalaba, al abordar la cesión de datos, era si el cesionario que recibe los datos puede tratar los datos, en virtud de un interés legítimo, cuando los datos han sido obtenidos sin legitimación adecuada por el cedente. Como se indicaba, la AEPD mantiene que la legitimación del cesionario se vería contaminada por la falta de legitimación del cedente[1074]. Sin embargo, no debería responsabilizarse al cesionario ignorante de esta falta de legitimación inicial del cedente, si este receptor de los datos actúa de acuerdo con lo que establece la legislación y pone a disposición del interesado los mecanismos para que pueda ejercer su poder de disposición respecto a los datos[1075].

Estos supuestos en los que parece que el responsable tendrá una mayor libertad al actuar en virtud de un interés legítimo que él mismo valora se contrarrestan con los mecanismos que establece la normativa para proteger los derechos de los afectados, como

---

[1073] R. MARTÍNEZ MARTÍNEZ, Olvidar es un fenómeno muy complejo, 14.5.2014 http://lopdyseguridad.es/olvidar-es-un-fenomeno-muy-complejo/ (fecha consulta: 21.8.2015).

[1074] La AEPD, en su Informe 111/2012 que versa sobre la aplicación del supuesto de legitimación relativo al interés legítimo, indica que "la legitimación del cesionario fundada en su interés legítimo sólo será posible si es legítimo el tratamiento llevado a cabo por su cedente, de forma que en caso de que el tratamiento sea ilícito en origen la mera invocación de un interés legítimo, aun cuando resulte prevalente, por el cesionario de los datos no implica que ese tratamiento devenga legítimo, por cuanto los datos habrían sido ilegítimamente sometidos a tratamiento en origen."

[1075] Según APARICIO SALOM el artículo 5.4 LOPD, al permitir que el responsable recoja datos personales que provengan de otras fuentes diferentes al propio interesado, con el único requisito de informar en un plazo de tres meses desde el registro de los datos, habilita a este responsable al tratamiento de estos datos. A este supuesto se le debería aplicar el art. 7.f) Directiva 95/46/CE que limitaría la disposición del 5.4 LOPD, de forma que cabrá tratamiento de datos si es necesario para la satisfacción del interés legítimo del responsable o del tercero a quien se comuniquen los datos, mientras no prevalezca el interés respecto de los derechos y libertades fundamentales del interesado que requieran protección. Si se cumple con estos requisitos, será indiferente que el cedente de los datos que recibe el responsable hubiera cometido una infracción al comunicar los datos. Si bien se excepcionaría si el responsable conociera de esta infracción y, de todas formas, siguiera con el tratamiento. J. APARICIO SALOM, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, 4ª Ed., *op. cit.*, págs. 203 a 207.

el deber de informar o los derechos ARCO. A estos mecanismos hay que sumar el contexto legal y constitucional, al que se somete el tratamiento que realiza el responsable. Ejemplo de ello, son disposiciones legales, como el artículo 25 LOPD, en sede de ficheros privados, que se refiere a su creación. Según indica este precepto, se podrá crear este tipo de ficheros, cuando ello resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que establece la ley para la protección de las personas. Por tanto, esta habilitación general al responsable se limita a una actuación en el marco de una actividad legítima.

Las comunicaciones sólo se permiten si responden al cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y del cesionario (art. 11 LOPD), por lo que también deben enmarcarse de acuerdo con estas funciones.

En el ámbito de las administraciones públicas, se establece la obligación de publicar la disposición general de creación, modificación o supresión de sus ficheros, de forma que se sometan al control de los ciudadanos y, más importante, se limita el tratamiento que puedan realizar a las competencias atribuidas legalmente (arts. 6, 20, 21 LOPD).

Desde una perspectiva de la protección constitucional, el legislador que establecerá, en su mayor parte, ese contexto que delimita el tratamiento, se haya sometido al necesario respeto de los requisitos que deben cumplir los límites al derecho fundamental de protección de datos. Por ello, en definitiva, el responsable, también debe tener en cuenta esta perspectiva constitucional que hará que, en ocasiones, se ponga en duda la validez de esas leyes. Además, el mismo responsable se encuentra en situaciones en que la ley le obliga a ponderar los diversos intereses y derechos en presencia, como el mencionado supuesto del interés legítimo.

5.3. El derecho a someter un código de conducta a las autoridades de control

La LOPD establece que, tanto los responsables del tratamiento del sector público, como del sector privado, puedan presentar estos códigos tipo que tendrán el carácter de códigos deontológicos o de buena práctica profesional y que deberán ser depositados en el Registro General de Protección de Datos o en los registros creados por las

Comunidades Autónomas (art. 32 LOPD que se desarrolla en el título VII RLOPD dedicado a los códigos tipo).

Estos códigos tienen carácter voluntario, pero serán vinculantes para quienes se adhieran a ellos (arts. 71.2 y 72.1 RLOPD). Se establece un contenido mínimo que deberán incluir los códigos y la posibilidad de añadir otros compromisos (arts. 73 y 74 RLOPD). Estos compromisos adicionales irán más allá del cumplimiento estricto de la ley[1076], de lo que se deriva que no es necesario que el código tipo tenga este plus, sino que lo que se pretende es que se facilite el cumplimiento de la normativa mediante una adaptación a una concreta problemática sectorial.

Es importante el establecimiento de las garantías del cumplimiento, ya que es realmente lo que convierte al código en algo más que una declaración de intenciones[1077]. El RLOPD exige que se incluyan procedimientos de supervisión que deben ser independientes y un régimen sancionador adecuado, eficaz y disuasorio (art. 75.1 RLOPD). Incluso, se podrán incorporar medidas de reparación en caso de haberse producido un perjuicio al afectado (art. 75.3 RLOPD)[1078].

Se distingue entre los códigos de carácter sectorial, aquellos que promueva una sola empresa y los que promuevan administraciones públicas (art. 72 RLOPD). En el primer caso, los códigos pueden referirse a la totalidad o a parte de los tratamientos que lleven a cabo las entidades del sector. En el segundo caso deben referirse a la totalidad de tratamientos que lleve a cabo la empresa. En el caso de las administraciones públicas y corporaciones de derecho público, solo se hace referencia a que podrán adoptar los códigos, de acuerdo con la normativa que les sea aplicable.

[1076] Ejemplo de estos compromisos son la adopción de medidas de seguridad adicionales a las exigidas por la normativa, la identificación de categorías de cesionarios o importadores de datos, medidas concretas de protección de menores o determinados colectivos o el establecimiento de un sello de calidad (art. 74 RLOPD).

[1077] No obstante, MALUQUER DE MOTES BERNET considera que los códigos de conducta son auténticas fuentes de derecho ya que pueden considerarse como costumbre. Se trata de un estilo, unos usos normativos, una forma de hacer que se crea en el marco de una comunidad de empresas y, en la medida que los asumen, son obligatorios para sus miembros. C. MALUQUER DE MOTES BERNET, "Códigos de conducta y buenas prácticas en la gestión de datos personales", M.R. LLÁCER MATACÁS, *Protección de datos personales en la sociedad de la información y la vigilancia*, La Ley, Las Rozas (Madrid), 2011, págs. 128 a 129.

[1078] Ver Capítulo VII.

Es necesario que el código tipo se deposite e inscriba en el Registro General de Protección de Datos (art. 77.1 RLOPD). Posteriormente al depósito, las entidades promotoras del código tipo deberán mantener accesible al público la información actualizada sobre las entidades promotoras, el contenido del código, los procedimientos de adhesión y de garantía y la relación de adheridos (art. 78.1.a) RLOPD). También deben remitir a la AEPD una memoria anual sobre las actividades realizadas que se relacionan con el código (difusión, verificación de cumplimiento, quejas, reclamaciones), así como evaluar periódicamente la eficacia del código. Se trata, por lo tanto, de una medida de autorregulación regulada, en la que no se deja en manos únicamente del responsable la adopción del código, sino que hay una tutela de la autoridad, que se asegura de que, realmente ese código respeta la normativa y que será eficazmente aplicado[1079].

De esta regulación se extraen algunas obligaciones que deben cumplir sujetos diferentes a los responsables del tratamiento y a los encargados del tratamiento: las entidades promotoras de los códigos tipo. Sin embargo, en caso de incumplimiento de estas obligaciones, no tendrían atribuida ninguna consecuencia en el marco sancionador de la LOPD.

Únicamente hay doce códigos tipo registrados en la AEPD (once registrados directamente y uno presentado en la Agencia Vasca de Protección de Datos)[1080]. La mitad son del sector sanitario y los otros son del sector de los seguros, de una asociación de municipios, del sector inmobiliario, de una universidad y el de "Confianza online". Éste último elaborado por la Asociación sin ánimo de lucro Confianza online es el más conocido ya que sirve para certificar sitios web[1081].

[1079] M.M. DARNACULLETA I GARDELLA, *Autorregulación y derecho público: la autorregulación regulada*, *op. cit.*, pág. 263. Asimismo, para GARCÍA MORALES, el punto clave en el diseño de estos mecanismos de autorregulacón es conseguir su efectividad, ya que su principal característica es la ausencia del poder coercitivo que tiene la regulación y su fundamento en la voluntariedad. M.J. GARCÍA MORALES, "Poderes públicos, autorregulación y protección del consumidor en Internet: a propósito de la regulación del distintivo público de confianza", L. COTINO HUESO (Coord.) VVAA, *Consumidores y usuarios ante las tecnologías*, págs. 269 a 270.

[1080] http://www.agpd.es/portalwebAGPD/canaldocumentacion/codigos_tipo/index-ides-idphp.php, (fecha consulta: 12.8.2014).

[1081] Si bien este sello contiene una parte dedicada a la protección de datos también se elaboró, en virtud de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (BOE núm. 166 de 12.7.2002) (LSSI). Esta ley preveía la posibilidad de adoptar códigos de conducta relativos a las materias que regulaba (art. 18). Además la LSSI incentivaba la adhesión a estos códigos, al contemplarlo como un criterio que podía graduar la sanción (art. 40 g). Por otro lado, la LSSI, en su

¿A qué puede responder este poco éxito en la elaboración de códigos tipo en España? La poca cultura de nuestro país en materia de autorregulación se debe a que, como en todo el continente europeo, se tiende a legislar de forma que se intentan cubrir todas las áreas[1082]. También puede deberse al hecho de que elaborar un código tipo requiere de un gran esfuerzo por parte de las organizaciones sectoriales que deben invertir recursos y, además, exige de un continuo mantenimiento. Sin duda, es esencial para incentivar el uso de estos instrumentos que se impulsen mecanismos de certificación que den la posibilidad a los responsables de sacar rédito de este esfuerzo con una mejora en su imagen[1083].

---

disposición final octava, establecía la aprobación por el Gobierno de un distintivo que debía permitir identificar a los prestadores de servicios que respetasen códigos de conducta adoptados con la participación del Consejo de Consumidores y Usuarios, y que incluyeran, entre otros contenidos, la adhesión al Sistema Arbitral de Consumo o a otros sistemas de resolución extrajudicial de conflictos que respetaran los principios establecidos en la normativa comunitaria sobre sistemas alternativos de resolución de conflictos con consumidores. Fruto de esta disposición se adoptó, primero el Real Decreto 292/2004, de 20 de febrero, por el que se crea el distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico y se regulan los requisitos y procedimientos de concesión, que posteriormente fue derogado por el Real Decreto 1163/2005, de 30 de septiembre, por el que se regula el distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico, así como los requisitos y el procedimiento de concesión. (BOE núm. 241 8.10.2005). Al código de Confianza online se le concedió este distintivo público mediante la Resolución de 15 de julio de 2005, del Instituto Nacional de Consumo, por la que se da publicidad a la concesión del distintivo público de confianza en línea (BOE núm. 255, 25.10.2005). En la fecha de consulta, 2.669 sitios web contaban con el sello Confianza online. https://www.confianzaonline.es/ (fecha consulta: 12.8.2014). Sobre el distintivo público de confianza, ver M.J. GARCÍA MORALES, "Poderes públicos, autorregulación y protección del consumidor en Internet: a propósito de la regulación del distintivo público de confianza", L. COTINO HUESO (Coord.) VVAA, *Consumidores y usuarios ante las tecnologías*, *op. cit.*.

[1082] GARCÍA MORALES resalta la poca tradición de la autorregulación en España pese a las claras ventajas especialmente en el contexto de Internet, donde se pueden utilizar para luchar contra los contenidos ilícitos y evitar una intervención estatal que pueda calificarse de censura. M.J. GARCÍA MORALES, "Capítulo I. Libertad de expresión y control de contenidos en Internet", P. CASANOVAS ROMEU (Ed.) *Internet y pluralismo jurídico: formas emergentes de regulación*, *op. cit.*, pág. 54.

[1083] *Ibídem*, pág. 57.

CAPÍTULO VII

EL RESPONSABLE Y LAS GARANTÍAS DEL DERECHO A LA PROTECCIÓN DE DATOS

Las garantías de los derechos fundamentales se pueden definir como el conjunto de medios que el ordenamiento prevé para la protección, tutela o salvaguardia de estos derechos[1084]. En el derecho a la protección de datos, el responsable juega un papel primordial respecto a la efectividad de estas garantías, ya que se encuentra en la primera línea de defensa del derecho. Como se verá en este capítulo, existe una tendencia, desde todas las ramas del derecho, a convertir al responsable si no en garantía, sí en necesario garante del derecho a la protección de datos.

La aproximación a las garantías y a su conexión con el responsable se iniciará con la regulación contenida en la Directiva 95/46/CE y se completará con la prevista en las leyes nacionales europeas que la han transpuesto, de forma que se detendrá especialmente en la legislación española. No obstante, en un sistema de protección de derechos fundamentales multinivel[1085], para tener una visión completa de las garantías, habrá que mencionar las que incluirán cada uno de los ordenamientos que conforman estos diferentes niveles[1086]. Al partir del análisis de la Directiva 95/46/CE, me centraré en garantías de tipo preventivo, como es el ejercicio de derechos ante el responsable, así como represivas, como son los recursos, la responsabilidad o las sanciones.

1. EL RESPONSABLE Y LAS GARANTÍAS PREVISTAS EN LA DIRECTIVA 95/46/CE

En el ámbito del Consejo de Europa, el Convenio 108 obliga, de una forma general, a los Estados parte a establecer sanciones y recursos contra las infracciones de las disposiciones de derecho interno que apliquen los principios de protección de datos

[1084] L. M. DÍEZ-PICAZO, *Sistema de derechos fundamentales*, 4ª ed., Aranzadi, Cizur Menor (Navarra), 2013, pág. 69.
[1085] T. FREIXES SANJUAN, "Els drets fonamentals en perspectiva multinivell. Reflexions entorn dels seus efectes", *Revista catalana de dret públic*, núm. 50, (juny 2015), pág. 34.
[1086] Realiza un recorrido por las garantías genéricas y específicas del derecho a la protección de datos en los diferentes sistemas europeos de protección de derechos fundamentales (Consejo de Europa, UE y ordenamientos nacionales europeos) M. ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa, op. cit.*, págs. 173 a 187, 339 a 374, 537 a 595.

(art. 10 Convenio 108). De acuerdo con la naturaleza no autoejecutiva del convenio, se aclara en el Informe explicativo del mismo, que serán los Estados parte los que determinen la naturaleza de estas sanciones y recursos (civil, administrativa, penal)[1087].

La Directiva 95/46/CE esboza un poco más las vías que los Estados miembros deberán instaurar para asegurar que sus ciudadanos posean las herramientas para poder reaccionar ante el incumplimiento de lo establecido en las normativas nacionales que transpongan la directiva. Este esbozo corresponde a los mecanismos que tradicionalmente proporcionan las diversas ramas del derecho. Así se incluye el recurso genérico a la justicia, la obtención de una compensación por los daños sufridos característica del derecho civil y el establecimiento de sanciones que respondería al carácter punitivo del derecho penal o del administrativo sancionador.

No obstante, antes de llegar a la sede judicial, el titular de los datos tendrá otras opciones: dirigirse ante el propio responsable para ejercitar los derechos de acceso, rectificación, cancelación u oposición y acudir a la autoridad de control, entidad encargada de la supervisión del cumplimiento de la normativa.

1.1. El ejercicio previo de derechos ante el responsable

Los derechos que la Directiva 95/46/CE brinda al interesado para hacer efectivo el poder de control sobre sus datos personales constituyen una herramienta esencial que éste tendrá para proteger su derecho. Este carácter esencial se reflejó mediante la incorporación expresa del acceso y la rectificación en el enunciado del derecho a la protección de datos en la Carta UE[1088]. Anteriormente, el Convenio 108 reconoció la naturaleza de garantía a estos derechos al incluirlos bajo la rúbrica "garantías complementarias para la persona concernida" (art. 8 Convenio 108).

Asimismo, el TJUE también ha resaltado el carácter instrumental que el ejercicio de estos derechos puede tener para asegurar, tanto el derecho al recurso judicial, como el

[1087] *Data protection compilation of Council of Europe texts, op. cit., Explanatory report Convention for the protection of individuals with regard to automatic processing of personal data*, apdo. 60.
[1088] "Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación" (art. 8.2 Carta UE).

derecho a obtener una indemnización (arts. 22 y 23 Directiva 95/46/CE)[1089]. Especialmente el derecho de acceso puede ayudar al afectado a obtener evidencias que obren en poder del responsable y que ayuden a la preparación de su estrategia procesal.

La Directiva 95/46/CE obliga a los Estados miembros a garantizar que estos derechos se ejercerán directamente ante el responsable de acuerdo con los procedimientos que se establezcan en las legislaciones nacionales. Por tanto, el responsable deberá cumplir con la obligación de atender estas peticiones y decidir si las concede o deniega. Para ello, será necesario que el responsable haya preparado su organización para atender eficazmente las peticiones y respetar los plazos que se determinen.

Hay que añadir que la Directiva 95/46/CE demanda al responsable que no se limite a actuar en el ámbito de su organización, sino que debe notificar a aquellos terceros a quienes haya podido comunicar previamente los datos la actuación que ha llevado a cabo respecto a los mismos para cumplir con lo preceptuado en la normativa (ya sea una rectificación, supresión o bloqueo de los datos). Sólo se permite la exoneración de esta obligación de notificación si resultara imposible o supusiera un esfuerzo desproporcionado.

Si el responsable decidiera atender la solicitud del interesado repararía la situación sin demora. Si el responsable respondiera negativamente o no respondiera a la solicitud del interesado, éste aún podría dirigirse a la autoridad de control para que supervisara la decisión del responsable y evidentemente a los tribunales por las vías previstas en el ordenamiento nacional.

Por tanto, el ejercicio de estos derechos ante el responsable se configura, de forma natural, como un paso previo o incluso preparatorio a la utilización de las garantías procesales. En este sentido, hay que indicar que en el Convenio 108 se ha previsto de

[1089] El TJUE considera que el derecho de acceso es indispensable para que el interesado pueda ejercer los derechos de rectificación, supresión o bloqueo de los datos o para solicitar del responsable que notifique a los terceros a quienes haya comunicado los datos que realicen estas acciones. Pero el TJUE además apunta a lo importante que es este derecho para que el interesado pueda ejercer el derecho de oposición contemplado en el artículo 14 Directiva 95/46/CE y para que ejerza el derecho a recurrir según se establece en los artículos 22 y 23 Directiva 95/46/CE. Para garantizar que estas disposiciones puedan ser útiles, además, indica el tribunal, que es necesario que el derecho de acceso se refiera al pasado, lo que no está tan claro es la extensión de este pasado. Sentencia del TJUE de 7 de mayo de 2009, *College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer*, C-553/07, EU:C:2009:293, apdos 51 a 55.

forma específica que, en caso de que no se atendieran estos derechos se obligue a los Estados parte a posibilitar que la persona concernida disponga de un recurso (art. 8.d) Convenio 108).

1.2. El recurso a las autoridades de control

La mención de la Directiva 95/46/CE a la posible habilitación de un recurso administrativo previo a la vía judicial que pudiera interponerse ante la autoridad de control (art. 22 Directiva 95/46/CE), debe completarse con lo que la misma Directiva dispone al respecto de las autoridades de control (Capítulo VI Directiva 95/46/CE).

Las autoridades de control se han configurado como parte esencial del derecho a la protección de datos, de forma que la Carta UE establece explícitamente que "el respeto de estas normas estará sujeto al control de una autoridad independiente" (art. 8.3 Carta UE). Uno de los principales requisitos que se extrae, por tanto, de este precepto es la independencia que debe caracterizar a las autoridades de control.

El TJUE, además de establecer que las autoridades de control son las guardianas de los derechos y libertades (como señala el Considerando 62 Directiva 95/46/CE) y un elemento esencial de la protección de datos, definió esta "total independencia" como aquel estatuto que garantiza la posibilidad de actuar con plena libertad, a resguardo de cualquier tipo de instrucciones o presiones[1090].

[1090] Según el TJUE, esta independencia supone una facultad de decisión exenta de toda influencia externa, ya sea directa o indirecta y trata de asegurar un control eficaz y fiable del respeto de la normativa, en materia de protección de datos. No supone, por tanto, según el TJUE, otorgar un estatuto particular a estas autoridades, sino reforzar la protección de las personas, por lo que estas autoridades deben actuar con objetividad e imparcialidad y, por ello, han de mantener esta independencia. Así lo manifestó el TJUE, en una sentencia en la que declaró que la República Federal de Alemania había incumplido con las obligaciones del artículo 28.1 Directiva 95/46/CE. La legislación de protección de datos alemana, ya hemos visto que diferencia entre el sector público y el privado. El sistema de supervisión también era diferente, según el sector. Respecto al sector público, las autoridades encargadas de controlar el respeto de esta normativa, solo respondían ante el respectivo Parlamento (según se tratara de una autoridad federal o las de los respectivos *Länder*). En cambio, en el sector privado, las autoridades de control estaban sometidas a la la tutela del Estado. Según Alemania, esta tutela no constituía una influencia externa, sino un mecanismo de vigilancia interna de la Administración, que llevaban a cabo autoridades, incardinadas dentro de la misma estructura administrativa que la autoridad de control, y obligadas también, a respetar los objetivos de la Directiva 95/46/CE. El TJUE afirma que la tutela del Estado permite al gobierno del *Land* influir en las decisiones de las autoridades de control. Aunque no fuera el objetivo perseguido por el gobierno del *Land*, este podría tener intereses en no respetar la normativa de protección de datos, respecto al sector privado, ya que podría ser parte interesada, por ejemplo, en una colaboración entre sector público y privado. Pese a que Alemania alegó que se trataba de un modelo que había aplicado desde hacía treinta años, el TJUE entiende

En lo que respecta a las herramientas que la Directiva 95/46/CE proporciona a estas autoridades para cumplir con sus objetivos son principalmente: poderes de investigación, poderes de intervención y capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la Directiva 95/46/CE o capacidad de poner en conocimiento de la autoridad judicial estas infracciones (art. 28.3 Directiva 95/46/CE). El ejercicio de estos poderes conlleva que los responsables deban someterse a ellos y, por tanto, genera para estos responsables obligaciones.

Las autoridades podrán ejercer estos poderes en el territorio de su propio Estado miembro, aunque también lo podrán hacer a instancias de otra autoridad (art. 28.6 Directiva 95/46/CE). En este sentido, se establece que las autoridades cooperen entre sí cuando sea necesario para cumplir sus funciones.

En la Directiva 95/46/CE también se especifica que las decisiones de las autoridades de control podrán ser objeto de recurso jurisdiccional (art. 28.3 *in fine* Directiva 95/46/CE), independientemente de que pueda acudirse también directamente ante los tribunales en caso de una posible vulneración del derecho a la protección de datos.

Las autoridades de control tienen una misión compleja, ya que, por un lado, brindan asesoramiento a los responsables del tratamiento, promueven el cumplimiento de la legislación y, por el otro, deben asegurarse de que se cumple y deben perseguir a quienes la incumplen. De este modo, se vuelven juez y parte, lo que hace que tengan un papel muy difícil de desempeñar. Por ello, se ha sugerido que deberían separarse bien las funciones de estos organismos[1091].

---

que las autoridades no contaban con la independencia promovida por la Directiva 95/46/CE. Sentencia del TJUE de 9 de marzo de 2010, *Comisión Europea c. República federal de Alemania*, C-518/07, EU:C:2010:125, apdos. 16, 18, 19, 23, 25, 35.

[1091] Así se indica en un estudio realizado, en el que se recomendaba incluso que las autoridades de control podrían quedarse con el papel de asesoramiento y dejar la aplicación de la normativa a los tribunales. *Comparative study on different approaches to new privacy challenges, in particular in the Light of technological developments, Contract _r: JLS/2008/C4/011 – 30-CE-0219363/00-28, Final report, LRDP KANTOR Ltd & Centre for Public Reform, European Commission, Directorate General Justice, Freedom and Security, 20.1.2010,* pág. 44.

Hay que resaltar la labor que realizan las autoridades de control europeas en el seno del GA29. Especialmente importante es el desarrollo de la línea interpretativa de las disposiciones de la Directiva 95/46/CE mediante la abundante documentación consistente principalmente en más de doscientos dictámenes o documentos de trabajo[1092]. Esta documentación ha adquirido gran relevancia y además de servir a los responsables para guiar su actuación, también sirve de pauta a las mismas autoridades de control y a los órganos judiciales que también hacen referencia a la misma, pese a no ser vinculante. Sin duda, esta doctrina ha sido un instrumento que las autoridades han utilizado para intentar minimizar las carencias y divergencias de la Directiva 95/46/CE.

Hay que puntualizar que, cuando los tratamientos de datos los lleven a cabo las instituciones u organismos comunitarios, el Reglamento 45/2001, norma aplicable en estos casos, ha creado una autoridad de control específica: el Supervisor Europeo de Protección de Datos (art. 1.2 y Capítulo V Reglamento 45/2001).

La importancia de las autoridades de control también se ha confirmado en el marco del Consejo de Europa. En el Convenio 108 se mencionaba la obligación de designar una o más autoridades, con el fin de que los Estados parte se prestaran la debida asistencia mutua (art. 13.2.a) Convenio 108). Sin embargo, la memoria explicativa del Convenio 108 aclaraba que esta designación no implicaba la creación de una autoridad de protección de datos[1093].

Con el fin de mejorar la aplicación de los principios enunciados en el Convenio 108 se aprobó un protocolo adicional que estableció la obligación de crear autoridades de control. De esta forma, se reconoció la importancia de estas entidades que la mayoría de Estados parte del Convenio 108 ya habían puesto en marcha[1094]. Así, la existencia de

[1092] El GA29 en un ejercicio de transparencia publica toda la documentación que emite (dictámenes, recomendaciones, guías, documentos de trabajo e incluso la correspondencia que mantiene). Se puede consultar esta documentación en: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm (Fecha consulta: 24.6.2015).

[1093] *Explanatory report Convention for the protection of individuals with regard to automatic processing of personal data, Data protection compilation of Council of Europe texts, op. cit.*, apdo. 73.

[1094] Así, se considera que estas autoridades "*have become and essential component of the data protection supervisory system in a democratic society*". *Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data regarding supervisory authorities and transborder data flows (Strasbourg, 8.11.2001), Explanatory report*, apdo. 5.

estas autoridades se considera que deriva de la obligación de adopción de sanciones y recursos apropiados (art. 10 Convenio 108)[1095].

El Convenio 108 establece que estas autoridades de control ejercerán sus funciones con independencia, que sus decisiones podrán ser recurridas judicialmente y que deberán cooperar con otras autoridades (art. 1, apdos. 3, 4 y 5 Protocolo adicional Convenio 108).

1.3. Mecanismos procesales

El derecho a un recurso efectivo ante los tribunales para proteger las violaciones de derechos fundamentales está reconocido a nivel internacional y, en concreto, a nivel europeo[1096]. Y es que, al hablar de un derecho fundamental, no sólo deberemos atender a lo que dispongan las leyes nacionales para proteger a sus titulares, sino a los cauces de protección establecidos a todos los niveles. No se puede olvidar, por tanto, el posible acceso por parte de los particulares al TJUE o al TEDH siempre que se cumplan los presupuestos necesarios[1097].

Así, una persona tiene la posibilidad de acudir al TJUE, tanto directa, como indirectamente, en virtud de las vías generales previstas en los tratados[1098]. Asimismo, si una institución u organismo comunitario incumpliera las disposiciones del Reglamento (CE) nº 45/2001, norma específica en materia de protección de datos respecto a los tratamientos de datos que realizan las entidades de la UE, también la persona afectada

[1095] *Ibídem*.
[1096] Este derecho se recoge en el artículo 8 de la Declaración Universal de Derechos Humanos aprobada en 1948, por Resolución de la Asamblea General de la ONU 217 A(III) del 10 de diciembre de 1948. Asimismo, a nivel europeo se establece en el ámbito de la UE el derecho a la tutela judicial efectiva en caso de violación de derechos o libertades garantizadas por el derecho de la UE (art. 47 Carta UE) y en el marco del Consejo de Europa, el derecho a un proceso equitativo (art. 6 CEDH).
[1097] Manual de legislación europea en materia de la protección de datos, Oficina de Publicaciones de la Unión Europea, 2014, http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-es.pdf (fecha consulta: 24.6.2015), págs. 134 a 139, que cita como ejemplo la Sentencia del TEDH de 17 de octubre de 2008, *I v. Finland*.
[1098] Toda persona física puede interponer recurso ante el TJUE contra los actos de los que sea destinataria o que le afecten directamente (art. 263 TFUE) Los particulares también podrán pedir en el marco de un procedimiento judicial nacional al tribunal nacional que solicite aclaración al TJUE sobre la interpretación del derecho europeo primario o derivado mediante la interposición de una cuestión prejudicial (art. 267 TFUE). Así, de forma indirecta las personas afectadas por una vulneración de su derecho a la protección de datos pueden forzar una interpretación del derecho europeo que les pueda favorecer en la protección de su derecho. Esta interpretación puede afectar al responsable si fuera quien ostentara la legitimación pasiva en el procedimiento nacional origen de la cuestión prejudicial. *Ibídem*, pág. 136.

podrá acudir al TJUE o al Supervisor Europeo de Protección de Datos (art. 32 Reglamento 45/2001 y art. 263 TFUE)[1099]. En este último caso, la decisión del Supervisor podrá recurrirse ante el TJUE (art. 32.3 Reglamento 45/2001). Si el particular es miembro del personal de una institución u organismo de la UE deberá recurrir al Tribunal de la Función Pública de la UE[1100].

En lo que se refiere al acceso al TEDH, desde el 1 de noviembre de 1998, cuando entró en vigor el Protocolo nº 11 del CEDH, se reconoció a los particulares legitimación activa para presentar demandas ante el TEDH (art. 34 CEDH)[1101]. Se puede acudir al TEDH por vulneración del derecho a la protección de datos (art. 8 del CEDH), aunque se deben cumplir los requisitos establecidos como el agotamiento de las vías de recurso nacional disponibles y que responda a criterios de admisibilidad (arts. 34 a 37 CEDH)[1102].

El responsable no será susceptible de ser parte en el proceso ante el TEDH. La legitimación pasiva la ostentará el Estado parte del CEDH en cuya jurisdicción se haya cometido la violación del derecho invocado[1103]. El responsable causante de la vulneración, en consecuencia, no podrá ser llevado ante el tribunal aunque será su conducta la que originará que se enjuicie al Estado. Si éste no ha cumplido con sus obligaciones positivas para adaptar su normativa interna a los compromisos contraídos al suscribir el CEDH y sus protocolos, y, por tanto, no ha asegurado la protección de los derechos fundamentales, será condenado. El Estado parte deberá ejecutar la sentencia del TEDH de forma que ponga fin a la vulneración y subsane las consecuencias negativas que haya sufrido el demandante[1104].

La Directiva 95/46/CE también refleja este derecho al acceso a la justicia específico para la materia que regula. En consecuencia, se establece la obligatoriedad para

[1099] *Ibídem*, pág. 138.
[1100] Protocolo (nº 3) del TFUE sobre el Estatuto del Tribunal de Justicia de la Unión Europea, Anexo I, art.1.
[1101] P. MORENILLA ALLARD, "La demanda de amparo ante el Tribunal Europeo de Derechos Humanos (I)", V. GIMENO SENDRA, P. MORENILLA ALLARD, *Los procesos de amparo. Civil, penal, administrativo, laboral, constitucional y europeo*, 3ª ed., Colex, Madrid, 2014, pág. 213.
[1102] *Ibídem*, págs. 231 a 241.
[1103] *Ibídem*, pág. 228.
[1104] Las sentencias del TEDH son declarativas y son los Estados condenados los que deben elegir los medios para cumplirlas. Sin embargo, por lo general las sentencias se cumplen de forma satisfactoria. P. MORENILLA ALLARD, "La demanda de amparo ante el Tribunal Europeo de Derechos Humanos (II)", V. GIMENO SENDRA, P. MORENILLA ALLARD, *Los procesos de amparo. Civil, penal, administrativo, laboral, constitucional y europeo*, *op. cit.*, pág. 258.

los Estados miembros de garantizar que toda persona disponga de un recurso judicial en caso de violación de los derechos garantizados por las disposiciones nacionales que se apliquen al tratamiento de datos (art. 22 Directiva 95/46/CE).

Durante el proceso de elaboración de la Directiva 95/46/CE se modificó el alcance de este recurso judicial. Inicialmente se pretendía proteger exclusivamente los derechos de acceso y oposición, pero al final se amplió el ámbito para que se pudiera utilizar, respecto a la violación de cualquiera de los derechos garantizados, sin especificar que se tratara únicamente de los mencionados[1105].

Por tanto, cabe deducir que la intención del legislador fue extender la protección de este recurso a todos los aspectos regulados en la legislación nacional, que transpone la Directiva 95/46/CE y que puedan considerarse derechos. Habrá que acudir a esta legislación nacional para ver si se han previsto los cauces procesales que cumplan este mandato.

Aunque no se mencione al responsable es evidente que la acción judicial deberá dirigirse contra éste, ya que será quien esté en posición de cesar en la conducta vulneradora.

[1105] En la Propuesta de Directiva de 1990 se establecía inicialmente que los Estados miembros debían instaurar un recurso judicial si los derechos de oposición, acceso, rectificación, borrado y bloqueo se infringían (art. 14.8 Propuesta de Directiva de 1990). Sin duda, esta previsión respondía al alineamiento con lo previsto en el Convenio 108. El Convenio 108 contempla la posibilidad de obtener la confirmación de la existencia o no en el fichero automatizado de datos de la persona concernida, así como de obtener la rectificación o el borrado de estos datos (art. 8 Convenio 108), es decir, lo que en la Directiva 95/46/CE correspondería al derecho de acceso. En caso de que no se atendieran estos derechos, como se ha indicado, se obliga a los Estados parte a posibilitar que la persona concernida disponga de un recurso (art. 8.d Convenio 108). Sin embargo, en el artículo 10 Convenio 108 también se indica que los Estados parte deben establecer las sanciones y recursos convenientes contra las infracciones de las disposiciones de derecho interno que hagan efectivos los principios básicos para la protección de datos establecidos en el Capítulo II del Convenio 108 (calidad, categorías particulares de datos, seguridad y las garantías complementarias indicadas). Por tanto, el Convenio 108 deja fuera de la previsión del establecimiento de sanciones y recursos la regulación de los flujos transfronterizos de datos. Esta exclusión es lógica si se tiene en cuenta que esta regulación lo que establece principalmente es la obligación de los Estados parte de no entorpecer estos flujos en aras de la protección de la vida privada. La posible intención de cubrir también esta previsión del artículo 10 Convenio 108 puede explicar que, en la Propuesta de Directiva de 1992 de la Directiva 95/46/CE, en su artículo 22, se ampliara la necesidad de contar con esta vía judicial para toda violación de los derechos previstos en la directiva y no sólo los que contemplaba el artículo 14. Este artículo 22 de la Propuesta de Directiva de 1992 además se incluyó en el capítulo III dedicado de forma genérica a los recursos judiciales, responsabilidad y sanciones.

1.4. Responsabilidad civil

El artículo 23 Directiva 95/46/CE establece el derecho que tiene toda persona que sufra un perjuicio derivado del tratamiento ilícito o de una acción incompatible con las disposiciones adoptadas en aplicación de la directiva, a obtener del responsable la reparación de este perjuicio. ¿Qué quiere decir tratamiento ilícito? ¿Y acción incompatible con las disposiciones nacionales?

La ilicitud del tratamiento en el ámbito de la Directiva 95/46/CE nos remite al Capítulo II de la misma, cuya rúbrica se refiere a las condiciones generales para la licitud del tratamiento de datos personales y que incluye el núcleo de la regulación de protección de datos. En consecuencia, es razonable deducir que si el tratamiento no respeta lo establecido en la normativa nacional que aplique el contenido de este capítulo de la Directiva 95/46/CE, será considerado un tratamiento ilícito. Quedan fuera, por tanto, de lo que cabría considerar tratamientos ilícitos, aquellos que incumplan la regulación de las transferencias internacionales, de los códigos de conducta y de las autoridades de control (Capítulos IV, V y VI Directiva 95/46/CE).

Otra cuestión más indeterminada será la mención a una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la Directiva 95/46/CE. Es apreciable el contraste con lo que se contempla en el precepto siguiente que hace referencia al régimen sancionador (art. 24 Directiva 95/46/CE). Así, se podrá aplicar una sanción en caso de incumplimiento de las disposiciones nacionales. Por tanto, el alcance de la responsabilidad civil es más amplio que el del régimen sancionador, ya que no es lo mismo una acción incompatible que un incumplimiento. Este alcance diferente en estos dos ámbitos es razonable debido a su naturaleza compensatoria, en el caso de la responsabilidad civil y punitiva, en el caso del régimen sancionador.

El establecimiento de este derecho a una indemnización plantea la cuestión de si hay que entender que esta disposición se refiere a una responsabilidad objetiva o subjetiva. Si acudimos al proceso de elaboración de la Directiva 95/46/CE, en el texto inicial se obligaba a los Estados miembros a establecer en la legislación nacional el derecho de los individuos, cuyos datos se almacenaran en un fichero y que sufrieran daños, como consecuencia del tratamiento o de cualquier conducta incompatible con la

Directiva, a obtener una indemnización del responsable (art. 21 Propuesta de Directiva de 1990).

Asimismo, se recalcaba que, en caso de incumplir la directiva, la responsabilidad ante el daño debía residir en la figura del responsable (Considerando 20 Propuesta 1990). No obstante, se eximía al responsable de esta obligación de indemnizar cuando el daño fuera resultado de la pérdida o destrucción de datos o del acceso no autorizado y el responsable probara que había adoptado las medidas de seguridad apropiadas (arts. 18 y 22 Propuesta de Directiva de 1990).

Por tanto, en esta primera versión de la Directiva 95/46/CE se apuntaba a una responsabilidad mixta. Claramente se establecía una responsabilidad objetiva, al disponer, en primer lugar, que la acción por daños y perjuicios se originaba por el perjuicio ocasionado por el simple tratamiento de datos o por una acción incompatible con las disposiciones de la directiva. No era preciso en este primer momento del trámite legislativo que el tratamiento fuera ilícito.

En segundo lugar, el responsable podría exonerarse de esta obligación de indemnizar si probaba que había actuado con la debida diligencia al cumplir con el deber de seguridad. Por tanto, en este caso, se planteaba una responsabilidad subjetiva en lo referente a este deber de seguridad, que exigía para generar la obligación de indemnizar la falta de diligencia. En consecuencia, debía entenderse que respecto a las otras obligaciones del responsable, no se proporcionaba la oportunidad de probar esta diligencia y debía indemnizarse en todos los casos, de forma que se trataría de una responsabilidad objetiva[1106].

[1106] El origen del artículo 23 Directiva 95/46/CE se encuentra, según HEREDERO HIGUERAS, en la sección 7 de la Ley federal alemana de 1990. En el debate que se produjo durante la elaboración del texto alemán que sustituiría la Ley federal de 1977, se consideró que el tratamiento de datos llevaba aparejado un riesgo inherente al mismo. Por tanto, la obligación de indemnizar hallaba su justificación en el hecho de utilizar una técnica que se consideraba lícita pero que era peligrosa, al igual que sucedía con los riesgos que acarreaba por ejemplo el uso de un vehículo, el suministro de electricidad o de gas. En este caso, se estimó que debía exigirse una responsabilidad por riesgo (*Gefärdungshaftung*) específica para este contexto aunque no existiera culpa o negligencia. M. HEREDERO HIGUERAS "Ensayo sobre la regulación de la responsabilidad y administrativa en la LO 15/1999 de protección de datos de carácter personal", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, *op. cit.*, págs. 2.178 a 2.185. El autor además remite en nota al pie a H. AUERNHAMMER, *Bundesdatenschutzgesetz*, Colonia, Heymann, 1981, págs. 88 a 89 y H.J. ORDEMANN, R. SCHOMMER, P. GOLA, *Bundesdatenschutzgesetz mit Erläuterungen*, 5ª ed., Beck, Múnich, 1981, págs. 130 a 140, para indicar que, en el seno de la comisión permanente de la Dieta federal

En la Propuesta de Directiva de 1992 se precisó que la acción de reparación se podía interponer si se sufriera un perjuicio como consecuencia de un tratamiento ilícito (art. 21.3 Propuesta de Directiva de 1992) y de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la directiva[1107]. Se introducía, por tanto, el adjetivo ilícito respecto al tratamiento. Se variaba la idea de que todo tratamiento implicaba una actividad que de por sí ya se consideraba generadora de un riesgo de provocar daños, para optar por la necesidad de que el tratamiento fuera ilícito para generar la obligación de indemnizar.

Sin embargo, se mantuvo la posible exoneración del responsable en el caso de haber adoptado las medidas de seguridad apropiadas. Por tanto, pese a que se exigía un tratamiento ilícito, sólo se mantenía la posibilidad de probar la diligencia debida en el caso del deber de seguridad.

Por último, la versión final de la Directiva 95/46/CE, en su artículo 23 mantiene la redacción de la versión de 1992 del primer apartado, pero se modifica la posibilidad de exoneración del responsable del tratamiento. De esta forma, no se admite la exención en los casos en los que los daños resulten de la pérdida o destrucción de datos o de un acceso no autorizado. La única posibilidad de que el responsable se exonere de esta obligación de indemnizar es si no se le puede imputar el hecho que ha provocado el daño (23.2 Directiva 95/46/CE). A título ejemplificativo, se mencionan como posibles supuestos que supondrían esta exoneración del responsable, que se demostrara la responsabilidad del interesado o que se diera un caso de fuerza mayor (Considerando 55 Directiva 95/46/CE).

---

se estimó, por tanto, necesario regular esta responsabilidad por riesgo. En la actual Ley alemana es la Sección 8 la que contempla esta responsabilidad objetiva que se refiere, al igual que sucedía en la ley de 1990, al sector público únicamente. De esta forma, esta Sección 8.1 Ley alemana establece: "*If a public body harms a data subject through collection, processing or use of his or her personal data which is unlawful or improper under this Act or other data protection provisions, the body's supporting organization shall be obligated to compensate the data subject for damage suffered irrespective of any fault.*" En cambio, la Sección 7 Ley alemana contempla el derecho a indemnización originado por un responsable del sector privado y establece, en la misma línea que la Directiva 95/46/CE, que la obligación de este responsable de indemnizar se origina por la recogida, tratamiento o uso de los datos personales de forma ilícita o contraria a lo establecido en la ley, con la única posibilidad de exonerar de la obligación al responsable cuando haya actuado diligentemente.

[1107] Así se corrigió la alusión que realizaba la Propuesta de Directiva de 1990 que se refería a la directiva en vez de a las disposiciones nacionales encargadas de transponer la regulación de la directiva.

El hecho de que en esta regulación se establezcan como únicas causas de exoneración de responsabilidad las relativas a la culpa de la víctima o fuerza mayor ha provocado que algún autor entienda que es un argumento para considerar que estamos ante una responsabilidad objetiva, ya que no admitiría que el responsable pudiera "exonerarse" si prueba su diligencia[1108].

Sin embargo, no puede vislumbrarse claramente el establecimiento de una responsabilidad objetiva, ya que no se refiere el artículo 23 Directiva 95/46/CE a la posibilidad de prescindir de la culpabilidad. La posible exoneración establecida también se puede conectar con una responsabilidad de naturaleza subjetiva si se entiende que las causas pueden referirse al componente de culpa[1109]. En conclusión, deberemos acudir a las disposiciones nacionales para ver cómo han hecho la transposición de este precepto y cómo se ha interpretado jurisprudencialmente.

Añadir al respecto de este derecho de indemnización que nada se incluye en la Directiva 95/46/CE sobre la responsabilidad por hecho ajeno que, por ejemplo pudiera jugar cuando la vulneración la realice el encargado del tratamiento o alguna persona

---

[1108] P. GRIMALT SERVERA, *La responsabilidad civil en el tratamiento automatizado de datos personales, op.cit.* pág. 162 y J.M. BUSTO LAGO, "La responsabilidad de los responsables de ficheros de datos personales y de los encargados de su tratamiento", *Revista Aranzadi Civil-Mercantil*, núm. 5, 2006, pág. 17. Hay que decir que HEREDERO HIGUERAS entiende que se trata de una responsabilidad objetiva. Sin embargo, a la hora de explicar lo que el autor considera como responsabilidad objetiva, se refiere a que la carga de probar que el daño no ha sido causado por su conducta es del causante del daño. M. HEREDERO HIGUERAS "Ensayo sobre la regulación de la responsabilidad y administrativa en la LO 15/1999 de protección de datos de carácter personal", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, págs. 2.178 a 2.185. Además, hay que tener en cuenta que la fuerza mayor y la culpa de la víctima se contemplan como causas de exoneración de responsabilidad en los sistemas de responsabilidad objetiva. Ver L.F. REGLERO CAMPOS, L. MEDINA ALCOZ, "Capítulo V. El nexo causal. La pérdida de oportunidad. Las causas de exoneración de responsabilidad: culpa de la víctima y fuerza mayor", L.F. REGLERO CAMPOS (Coord.), VVAA, *Tratado de responsabilidad civil, Tomo I Parte General*, 4ª ed., Aranzadi, Cizur Menor (Navarra), 2008, págs. 822 a 919.

[1109] Así, LLÁCER MATACÁS estima que las exoneraciones del Considerando 55 Directiva 95/46/CE avalan que se pueda defender respecto a lo que establece la LOPD el principio de imputación subjetiva del daño del artículo 1902 Cc. M.R. LLÁCER MATACÁS, *La autorización al tratamiento de información personal en la contratación de bienes y servicios. La privacidad, entre el estatuto del responsable y la fragilidad del consentimiento*, Dykinson, Madrid, 2012, pág. 121. En este sentido, en nuestro ordenamiento hay que recordar que el caso fortuito y la culpa concurrente de la víctima también se han entendido como causas de exclusión o reducción de la culpabilidad. Sólo puede responderse de aquellos sucesos que no hubieran podido preverse, o que, previstos, fueran inevitables (art. 1.105 Cc) de forma que no podrá considerarse que el causante del daño es negligente si el suceso que origina el daño no hubiera podido preverse o fuera inevitable. La culpa concurrente de la víctima también puede originar un juicio sobre las culpas de víctima y causante para valorar en consonancia el deber de indemnizar. L. DÍEZ-PICAZO, *Fundamentos del derecho civil patrimonial. V La responsabilidad civil extracontractual*, Aranzadi, Cizur Menor (Navarra), 2011, págs. 280 a 281.

autorizada por el responsable a tratar los datos de carácter personal. Por ello, habrá que acudir a la legislación nacional, aunque, en principio, lo que se observa en la Directiva 95/46/CE es una atribución de responsabilidad al responsable del tratamiento en todos los casos de vulneración de la regulación.

Por último, hay que mencionar, que, en el ámbito de la UE existe la posibilidad de reparación de los daños causados por sus instituciones o sus agentes en el ejercicio de sus funciones (art. 340 TFUE). En el ámbito del Consejo de Europa, el TEDH tiene la capacidad de otorgar una compensación económica si considera que ha existido violación del derecho a la protección de datos y el derecho interno del Estado condenado no permite reparar las consecuencias de esta violación[1110].

1.5. Régimen sancionador

En el texto inicial del proceso de elaboración de la Directiva 95/46/CE se obligaba a los Estados miembros a que establecieran sanciones disuasorias para asegurar el cumplimiento de las medidas establecidas en la directiva (art. 23 Propuesta de Directiva de 1990). En el texto de 1992 se precisó que estas sanciones se podrían aplicar a cualquier persona (art. 25 Propuesta de Directiva de 1992) ya fuera de Derecho privado o de Derecho público (Considerando 24 Propuesta de Directiva de 1992).

En el texto definitivo de la Directiva 95/46/CE se mantiene el establecimiento de las sanciones pero se amplía la posibilidad para los Estados miembros de adoptar otro tipo de medidas para garantizar el cumplimiento de lo establecido en la directiva (art. 24 Directiva 95/36/CE). Asimismo, se conserva la especificación de que la sanción se podrá

[1110] El artículo 41 CEDH establece que en caso de que el TEDH declare que ha habido violación del Convenio o de sus protocolos y si el derecho interno del Estado parte sólo permite de manera imperfecta reparar las consecuencias de dicha violación, el Tribunal concederá a la parte perjudicada una satisfacción equitativa. Ver ejemplos de sentencias en las que existe reconocimiento de indemnización en supuestos relativos al artículo 8 CEDH relacionados con el derecho de protección de datos en D. ORDÓÑEZ SOLÍS, *Privacidad y protección judicial de los datos personales*, Bosch, Barcelona, 2011, págs. 219 a 222. En el asunto *I v. Finland*, el TEDH considera que debe indemnizarse a la recurrente con 8.000 euros porque el Estado no había sido capaz de adoptar las medidas necesarias para garantizar la seguridad de la historia clínica de ésta en un hospital. En el procedimiento civil nacional, la recurrente no había podido probar la relación de causalidad entre la falta de adopción de medidas de seguridad y la difusión ilícita de sus datos clínicos. No obstante, el TEDH entendió que atribuir a la recurrente la carga de probar esta conexión no podía significar dejar pasar las deficiencias del hospital en materia de medidas de seguridad, de forma que para el tribunal lo esencial fue que resultó probado que el hospital había incumplido con su obligación de seguridad, establecida en la ley nacional. Sentencia del TEDH de 17 de octubre de 2008, *I v. Finland*, apdos. 44, 53 a 55.

imponer a toda persona, tanto de derecho privado como de derecho público (Considerando 55 Directiva 95/46/CE).

Pese al margen discrecional de los Estados miembros en la adopción de sanciones, el TJUE se pronunció al respecto en el asunto *von Colson*, de forma que exigió que en los casos en que se adoptara esta previsión en una directiva, la sanción que se determinara en la ley nacional que la transpusiera, debería ser adecuada para conseguir el objetivo perseguido por la directiva[1111].

2. EL RESPONSABLE Y LA TRANSPOSICIÓN DE LAS GARANTÍAS DE LA DIRECTIVA 95/46/CE EN LOS ORDENAMIENTOS EUROPEOS

En el primer informe del año 2003 que se elaboró sobre la implantación de la Directiva 95/46/CE en los Estados miembros en lo referido al grado de cumplimiento, la Comisión Europea aludía a tres factores que se interconectaban para dar como resultado un escaso nivel de cumplimiento. Estos tres factores eran: los limitados recursos de que disponían las autoridades de control para la aplicación de la normativa frente a la complejidad de las funciones que debían desempeñar; el escaso cumplimiento por parte de los responsables, lo que se achacaba al carente interés en cambiar sus prácticas para cumplir lo que estimaban requisitos muy complicados, cuando además el riesgo de asumir alguna consecuencia era enormemente bajo y, por último, el desconocimiento por parte de los titulares de los datos de sus derechos[1112].

[1111] En el asunto *von Colson*, un caso de discriminación, el TJUE analizó si la previsión de una directiva que imponía a los Estados miembros que estableciesen una vía jurisdiccional para las personas que se pudieran sentir perjudicadas por discriminación, se cumplía al prever una indemnización consistente en un pago simbólico (sólo incluía los gastos de desplazamiento ocasionados a las personas que aspiraban a un puesto de trabajo que les fue denegado por ser mujeres). El TJUE indicó que "los Estados miembros están obligados a adoptar medidas suficientemente eficaces para alcanzar el objetivo perseguido por la Directiva y hacer que estas medidas puedan ser invocadas efectivamente ante los Tribunales nacionales por las personas interesadas." Si bien el TJUE señala que la Directiva no imponía una sanción determinada, la ejecución completa de la misma implicaba, no obstante, que dicha sanción pudiera garantizar una protección jurisdiccional efectiva y eficaz. Además, debía tener un efecto disuasorio real respecto del empresario. "De ello resulta que cuando el Estado miembro elige sancionar las violaciones de la prohibición de discriminación por medio de una indemnización, ésta debe ser en todo caso adecuada al perjuicio sufrido." Por lo tanto, el tribunal rechaza que esta indemnización pueda ser puramente simbólica. Sentencia del TJUE de 10 de abril de 1984, *Sabine von Colson et Elisabeth Kamann c. Land Nordrhein-Westfalen*, C-14/83, EU:C:1984:153, apdos. 18 y 23.

[1112] *Report from the Commission, First report on the implementation of the Data Protection Directive 95/46/EC, COM(2003) 265 final, Brussels, 15.5.2003*, pág. 12.

Por tanto, las autoridades, los responsables y los titulares son los tres ejes alrededor de los que deben girar las posibles soluciones o medidas que garanticen la aplicación de la normativa y, en definitiva, la protección del derecho. Los tres deben coadyuvar para asegurar el cumplimiento. Y, a mi juicio, el legislador se ha dado cuenta que es esencial que el responsable se vea motivado al cumplimiento, ya sea por mecanismos punitivos, reparadores o preventivos. Son estos últimos los que se están incentivando, con el fin de evitar, en la medida de lo posible, el incumplimiento.

2.1. El ejercicio previo de derechos ante el responsable

El TC caracterizó al derecho de la protección de datos por su contenido consistente en la atribución a su titular de un haz de facultades que imponían a terceros (los responsables) deberes jurídicos que permitieran garantizar a ese individuo el poder de control sobre sus datos[1113]. Entre estas facultades se incluían el derecho de acceso, como derecho a saber en todo momento quién dispone de los datos y el uso al que los somete, el derecho a rectificar y el derecho a cancelar o a oponerse a esa posesión y usos[1114].

De esta forma, se puede afirmar que los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) que establece la LOPD son parte de este haz de facultades que menciona el TC. Estas facultades, a su vez, constituyen garantías que permiten asegurar ese poder de disposición sobre los datos.

Por tanto, estas facultades son un mecanismo que permite al titular de los datos dirigirse directamente al responsable y asegurar una restitución en su derecho, sin necesidad de acudir a otra instancia[1115]. El responsable debe responder la solicitud que le dirija el afectado, aunque no tuviera datos personales del mismo (art. 25.2 RLOPD).

[1113] STC 292/2000, de 30 de noviembre de 2000, FJ 6.
[1114] *Ibídem*.
[1115] La solicitud de ejercicio de estos derechos debe dirigirse al responsable y, en caso de que se dirigiera a un encargado del tratamiento, éste deberá trasladarla al responsable, a no ser que se hubiera pactado que el encargado atendiera estas solicitudes por cuenta del responsable (art. 26 RLOPD). Como se indicó en el Capítulo V, en algunas leyes nacionales también se ha establecido la posibilidad de intermediación en el ejercicio de derechos, como en el caso del ejercicio del derecho de acceso a datos sanitarios que se realizará a través de un médico que elija el interesado (art. 11.5 Ley portuguesa, art. 13.4 Ley rumana, art. 11.3 Ley de Liechtenstein), posibilidad que además permite el Considerando 42 Directiva 95/46/CE.

Sin embargo, la posibilidad de ejercer estas facultades no implica que sea un paso previo necesario para poder interponer cualquier acción judicial o dirigirse a la autoridad de control si se considera que existe una vulneración del derecho o un incumplimiento de la normativa. Asimismo, la no atención de la solicitud de ejercicio de derechos por parte del responsable o la denegación de la misma, pueden ser denunciadas ante la AEPD que iniciará un procedimiento denominado de tutela de los derechos (art. 18 LOPD).

2.2. El recurso a las autoridades de control

2.2.1. Las autoridades de control

En España, el TC ha considerado que las autoridades de control constituyen la dimensión institucional del régimen de protección de datos y que tienen una función de carácter tuitivo o preventivo[1116]. Además de la AEPD y tras la supresión de la Agencia de Protección de Datos de la Comunidad de Madrid, hay dos agencias autonómicas: la ACPD y la Agencia de Protección de Datos Vasca. Asimismo, hay que recordar la labor del Defensor del pueblo, tanto a nivel estatal como autonómico, de supervisión de los poderes públicos con el fin de defender los derechos fundamentales (art. 54 CE)[1117].

En la LOPD se especifica que la AEPD es un ente de derecho público, con personalidad jurídica propia, plena capacidad pública y privada y que actúa con plena independencia de las administraciones públicas. En este sentido ha sido muy discutida la cuestión de la independencia de la agencia, ya que el Director de la AEPD, máximo órgano de la misma, es nombrado por el Gobierno a propuesta del Ministro de Justicia de entre los miembros del Consejo Consultivo, otro órgano de la AEPD, por un período de cuatro años[1118]. El Director de la Agencia Vasca de Protección de Datos lo nombra el Gobierno Vasco por decreto por un período de cuatro años[1119].

[1116] STC 290/2000, FJ 8.

[1117] De hecho, la LOPD establece la obligación a la AEPD de comunicar al Defensor del Pueblo las resoluciones de declaración de infracción de las Administraciones Públicas (art. 46.4 LOPD). De hecho, la AEPD, en sus memorias, siempre incluye un apartado sobre la colaboración que lleva a cabo con los defensores del pueblo que suelen poner en conocimiento de la misma denuncias o quejas de los ciudadanos. Ver por ejemplo la Memoria de 2014 de la AEPD, pág. 98.

[1118] Artículo 35.1 LOPD, y artículos 1, 14,16 Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos (BOE núm. 106, 4.5.1993). La AEPD se compone del Director de la AEPD que es el que ejerce todas las funciones de la entidad y, por tanto, dicta todas las resoluciones e instrucciones que requiera el ejercicio de las funciones, el Consejo Consultivo, órgano que

En cambio, el Director de la ACPD lo designa el pleno del *Parlament* por mayoría de tres quintas partes o si no se obtuviera por la mayoría absoluta en segunda votación, a propuesta de *Consell Assessor de Protecció de Dades* (el equivalente al Consejo Consultivo de la AEPD) por un período de cinco años[1120].

La Directiva 95/46/CE otorgaba a las autoridades de control los poderes de investigación, intervención y la capacidad procesal[1121]. Pues bien, en el caso de los poderes que la LOPD otorga a la AEPD se le han atribuido claramente los dos primeros. Así, el TC afirmaba que la función preventiva de la AEPD se correspondía con la atribución de capacidades de control e intervención, registrales y consultivas. Asimismo, la AEPD dispone de las potestades administrativas de investigación o inspección, sancionadora, de resolución de reclamaciones por incumplimiento de la ley y normativa limitada a la posibilidad de dictar instrucciones[1122].

---

asesora al Director y dependiendo del Director: el Registro General de Protección de Datos, la Inspección de Datos y la Secretaría General. El artículo 16 Real Decreto 428/1993 se refiere específicamente a la independencia del Director de la AEPD, de forma que especifica que desempeñará su cargo con dedicación absoluta, plena independencia y total objetividad y no estará sujeto a mandato imperativo, ni recibirá instrucciones de autoridad alguna. Además se establecen en el artículo 15 Real Decreto 428/1993 las causas de cese y separación. En el estudio realizado por la FRA sobre las autoridades de control, se concluía que la autoridad de control española se podía considerar como independiente, ya que la elección del director se realizaba entre los miembros del Consejo consultivo, que eran elegidos por diferentes entidades que representan al conjunto de la sociedad, como el Consejo Superior de Universidades. También se consideró como un factor que denotaba independencia el hecho de que la AEPD gozara de personalidad jurídica. Entre otros factores a tener en cuenta para determinar el grado de independencia de las autoridades, este estudio destaca: la forma de designación y de remoción de los miembros de la autoridad (por ejemplo en Irlanda el gobierno puede remover a los comisionados, por lo que fallaría en este caso este aspecto); la autonomía financiera de la autoridad; la personalidad jurídica distinta; la capacidad procesal; la configuración constitucional de la garantía institucional (por ejemplo en Portugal y Grecia). *Data protection in the European Union: the role of national data protection authorities, strengthening the fundamental rights architecture in the EU II, op. cit.*, págs. 19 a 20.

[1119] Artículo 15.1 Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos (BOPV núm. 44 de 4.3.2004 y BOE núm. 279 de 19.11.2011)

[1120] Artículo 7.3 Ley catalana. Como indica MITJANS PERELLÓ esta designación parlamentaria responde al establecimiento del requisito de independencia respecto a la autoridad en el artículo 31 del Estatuto de Autonomía de Cataluña y diferencia a esta autoridad de control de las otras (la AEPD y la autoridad vasca). También a enfatizar este carácter independiente responde el cambio de denominación de la autoridad previsto en la Ley catalana, que pasó de agencia a autoridad, ya que habitualmente las agencias son entidades cuyo rasgo distintivo no es la independencia. E. MITJANS PERELLÓ, "El modelo de protección de datos de la Ley 32/2010, de 1 de octubre de 2010, de la Autoridad Catalana de Protección de Datos", *Comunicaciones en propiedad industrial y derecho de la competencia*, *op. cit.*, págs. 9 a 10.

[1121] No se incluye la potestad sancionadora. Las sanciones, que se contemplan en el artículo 24 Directiva 95/46/CE no requieren que sean las autoridades de control las que las impongan. Se deja margen de actuación a los Estados miembros para que decidan cómo establecerlas,

[1122] STC 290/2000, de 30 de noviembre de 2000, FJ 8,9.

La capacidad procesal que menciona la Directiva 95/45/CE debe entenderse referida a la legitimación activa para interponer acciones ante las infracciones de las leyes de protección de datos[1123]. No se menciona nada al respecto ni en la LOPD ni en el estatuto de la AEPD ni en las normativas autonómicas respecto a las agencias catalana y vasca[1124]. Además, sobre esta cuestión, el TC se manifestó al denegar a la AEPD la legitimación para interponer un recurso de amparo, en el asunto de la cancelación de datos personales en libros bautismales. El TC entendió que la AEPD no tenía interés legítimo por no poder esgrimir ni el derecho de tutela judicial efectiva cuando defendía el ejercicio de una potestad pública ni el derecho a la protección de datos del ciudadano afectado, ya que se trataba de un derecho fundamental ajeno[1125]. No todas las autoridades de control tienen las mismas potestades en todo el conjunto de normativas de la Unión Europea. De esta forma, se les otorga esta legitimación a las autoridades de Austria, Croacia, Francia, Hungría, Letonia, Lituania, Malta y Rumanía[1126].

Los poderes de investigación se reflejan en la potestad de inspección reconocida por el artículo 40 LOPD. El ejercicio de esta potestad corresponde a un órgano concreto de la AEPD: la Inspección de Datos. En el ámbito autonómico la normativa vasca contempla en la estructura orgánica de la agencia órganos que desempeñen las funciones

[1123] La Directiva 95/46/CE se refiere a "capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial" (art. 28.3 Directiva 95/46/CE).

[1124] Hay que especificar que me refiero a la capacidad procesal como posibilidad de actuar ante la autoridad judicial en caso de infracción de la normativa de protección de datos como sujeto con legitimación activa y no meramente para defender su actuación administrativa.

[1125] Se trató de un intento de la AEPD por atacar la polémica STS de 19 de septiembre de 2008 (Sala 3ª) (ROJ: STS 4646/2008) en la que el Alto Tribunal consideró que los libros bautismales no eran ficheros de acuerdo con la legislación de protección de datos y, por lo tanto, no procedía atender la solicitud de anotación en la partida de bautismo de la petición de cancelación de la persona que recurrió a la AEPD en procedimiento de tutela. Hay que tener en cuenta que fueron muchas las personas que reclamaban su derecho a cancelar los datos en estos libros con el fin de reflejar su calidad de apóstatas. La AEPD interpuso recurso de amparo ante el TC en base a la presunta vulneración de su derecho a la tutela judicial efectiva o, en todo caso por la vulneración del derecho a la protección de datos de la persona afectada. El TC estimó que la AEPD carecía de legitimación activa, ya que pese a haber sido parte en los procedimientos judiciales impugnados, no se consideraba que ostentara un interés legítimo. El TC consideró que no podía estimarse que el derecho a la tutela judicial efectiva otorgara a las entidades públicas este derecho en defensa de sus potestades públicas. Tampoco entendió el TC que la AEPD pudiera alegar la defensa del derecho a la protección de datos del recurrente ya que se trataba de un derecho ajeno y no le proporciona tampoco el interés legítimo necesario. Por último decir, que el magistrado don Pablo Pérez Tremps emitió voto particular en el que manifestó su discrepancia con el auto. ATC 20/2011, de 28 de febrero de 2011.

[1126] Esta capacidad procesal se establece en el Parágrafo 30 Ley austríaca; artículo 34 Ley croata; artículo 45.III Ley francesa; Sección 70 Ley húngara: artículo 29.4 Ley letona; artículo 41 Ley lituana; artículo 40 Ley de Malta y artículo 25.8 Ley rumana.

de asesoría, instrucción, inspección, secretaría y registro[1127]. Respecto a la ACPD, se establecen también unidades que dependen del director, entre las que figura la de inspección[1128].

Las inspecciones pueden realizarse de oficio o a instancia de los titulares de datos, en el marco de la etapa de instrucción de los procedimientos que pueden iniciarse ante la AEPD[1129]. El Tribunal Supremo ha reconocido la legitimación activa del titular de los datos denunciante para exigir que la AEPD desarrolle la actividad investigadora para la debida averiguación de los hechos denunciados[1130].

El ejercicio de la potestad de inspección conlleva que el responsable esté obligado a permitir el acceso a sus locales y atender las solicitudes de los funcionarios en referencia a sus documentos, equipos y sistemas informáticos donde se puedan tratar datos[1131].

[1127] Artículo 10 Decreto 309/2005, de 18 de octubre, por el que se aprueba el Estatuto de la Agencia Vasca de Protección de Datos (BOPV núm. 213 de 9.11.2005).

[1128] Los órganos de gobierno son el director o directora y el *Consell Assessor de Protecció de Dades* y del director dependen las unidades de Secretaría General, Asesoría jurídica, Área del Registro de Protección de Datos y Área de inspección. Respecto a la potestad de inspección se establece la posibilidad de que los funcionarios que la ejercen puedan ser auxiliados por personal no funcionario. Artículos 6, 19 Ley catalana y artículo 16 Decreto 48/2003, de 20 de febrero por el que se aprueba el Estatuto de la *Agència Catalana de Protecció de Dades* (DOGC núm. 3835 de 4.3.2003).

[1129] Respecto a las inspecciones, hay que decir que también se han utilizado como un instrumento de concienciación, mediante los llamados Planes Sectoriales de Oficio en los que se seleccionaba un sector que tuviera una gran problemática en materia de protección de datos. En la normativa catalana hay un equivalente que son los planes de auditoría (art. 20 Ley catalana). Se escogían algunos responsables de este sector y se realizaba una inspección que daba como resultado unas recomendaciones dirigidas al sector para facilitar el cumplimiento de la normativa y para sensibilizar al sector. Las recomendaciones resultantes se publican en el sitio web de la AEPD. Entre los sectores objeto de estas inspecciones está el de videovigilancia, sanidad, telefonía, seguros y solvencia patrimonial. http://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/index-ides-idphp.php (fecha consulta 17.6.2014).

[1130] Esto no implica que el denunciante pueda demandar que esa actividad necesariamente finalice en una resolución sancionadora, ya que la imposición de una sanción no produce ningún efecto positivo en la esfera jurídica del denunciante, por lo que no se le reconoce ningún interés real exigido para que fuera apreciada la legitimación. STS de 9 de junio de 2014 (Sala 3ª) (ROJ: STS 2365/2014), FJ 4, que recoge la doctrina contemplada en sentencias anteriores.

[1131] La regulación de las funciones de la Inspección de Datos se halla en los artículos 27 a 29 del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos. Hay que indicar que el artículo 28.2 de este Real Decreto establece específicamente que el sujeto obligado a permitir el acceso a sus locales es el responsable del fichero, por lo que, en principio, quedarían fuera el responsable del tratamiento y el encargado del tratamiento. Esta norma fue aprobada en 1993 y hace referencia a la LORTAD de 1992, por lo que debe entenderse que hay que ampliar el alcance a estos sujetos. Además, en ocasiones, podría ser necesario que la AEPD inspeccione locales de entidades que después de realizada la instrucción no se consideraran responsables. Respecto a la normativa autonómica en la vasca se menciona al responsable del fichero cuando se indica que se le deberá exhibir autorización del Director de la Agencia Vasca de Protección de Datos para poder acceder a los locales en los que se hallen los ficheros y equipos informáticos (art. 11.2 Decreto 309/2005). La normativa catalana establece de forma

En lo referido a los poderes de intervención, en su mayoría se conectan con la potestad sancionadora, como la potestad de inmovilizar ficheros que podrá llevarse a cabo en caso de infracciones graves o muy graves o la amonestación a los responsables (arts. 49 y 45.6 LOPD). Sin embargo, hay que indicar que no se han trasladado a la legislación española los controles previos que regula el artículo 20 Directiva 95/46/CE y que se citan como ejemplo de estos poderes de intervención (art. 28.3 Directiva 95/46/CE)[1132].

2.2.2. El procedimiento de tutela de derechos

Además de los procedimientos relativos al ejercicio de la potestad sancionadora, que se abordarán más adelante, el artículo 18 LOPD ubicado en el Título dedicado a los derechos de las personas estableció un procedimiento específico: la tutela de los derechos[1133]. Este procedimiento otorga la posibilidad al titular de los datos que hubiera ejercido los derechos de acceso, rectificación, cancelación u oposición (derechos ARCO) y a quien se le hubieran denegado total o parcialmente, de poder comunicarlo a la AEPD que supervisaría si la denegación del responsable era procedente.

No obstante, el precepto induce a dudas sobre el ámbito del procedimiento, ya que, inicialmente indica que "las actuaciones contrarias a lo dispuesto en la presente ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine" (art. 18.1 LOPD). Este apartado ha dado lugar a que se interpretara que el procedimiento podía utilizarse para denunciar cualquier conducta que incumpliera la ley[1134].

---

neutra sin establecer el sujeto inspeccionado concretamente (art. 19 Ley catalana y art. 20 Decreto 48/2003).

[1132] No se ha establecido, por tanto, la necesidad de que se examinen de forma previa por la autoridad de control los tratamientos que puedan suponer un riesgo específico para los derechos y libertades de los interesados.

[1133] El procedimiento se desarrolla además en los artículos 117 y siguientes del RLOPD. En virtud de su ubicación en el Título III dedicado a los "Derechos de las personas" reviste carácter de ley orgánica (ex Disposición final segunda LOPD), a diferencia de la regulación del Título VIII referido a "Infracciones y sanciones", donde se regula el procedimiento sancionador (art. 48 LOPD), que tiene carácter de ley ordinaria.

[1134] Así lo ha entendido M. VIZCAÍNO CALDERÓN, *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, pág. 215. SAN JOSÉ AMAT entiende que parece más ajustado a la voluntad del legislador entender que el procedimiento de tutela de derechos se refiere a los derechos ARCO, de forma que resalta su naturaleza de derechos singulares que se diferencian así del resto de derechos y principios que incluye la LOPD como el de información (art. 5 LOPD). C. SAN JOSÉ AMAT, "Tutela de los derechos", A. TRONCOSO REIGADA, (Dir.), VVAA, *Comentario a la Ley Orgánica de*

Sin embargo, los siguientes apartados del precepto se reconducen hacia un procedimiento centrado en el ejercicio de los derechos ARCO, lo que también es coherente con una interpretación sistemática.

Asimismo, esta interpretación se ha confirmado con la práctica[1135] y con el establecimiento en el RLOPD de la regulación del procedimiento de tutela de derechos dirigido de forma específica a los derechos ARCO[1136]. La posibilidad de acudir a la autoridad de control completaría la garantía que representan los derechos ARCO con dos posibles fases: el ejercicio ante al responsable y la supervisión de la autoridad. En caso de no obtener el resultado deseado si, por ejemplo, el responsable tampoco atendiera la solicitud de la AEPD, aún quedaría la posibilidad de iniciar un procedimiento sancionador contra este responsable[1137].

Protección de Datos de Carácter Personal, op. cit., págs. 1.241 a 1.245. No obstante, SAN JOSÉ AMAT cita una sentencia del Tribunal Supremo (STS de 28 de diciembre de 2004 (Sala 3ª) (ROJ STS 8494/2004), FJ 2) como argumento a favor de que la postura contraria: que el procedimiento sirva para ejercer todos los derechos concedidos por la LOPD. En esta sentencia se planteaba si el recurrente en casación, denunciante en el procedimiento ante la AEPD, tenía legitimación activa para discutir el sobreseimiento dictado por la AEPD. El Tribunal Supremo se remitió al artículo 17 LORTAD para defender la legitimación activa del denunciante, concluyó que debían anularse las actuaciones administrativas y obligó a la AEPD a iniciar las actuaciones oportunas para investigar los hechos denunciados. Por tanto, como la denuncia se refería a una cesión de datos y el Tribunal Supremo alegó el artículo 17 LORTAD como argumento a favor de la legitimación, entiende SAN JOSÉ AMAT que esta disposición incluiría cualquier reclamación contra un incumplimiento de la LORTAD, en ese momento, y actualmente de la LOPD. Sin embargo, no se puede equiparar el contenido del 17 LORTAD y el actual 18 LOPD, ya que el precepto de la LORTAD era más ambiguo. El artículo 17 incluía en el mismo precepto la regulación de la "Tutela de los derechos y derecho de indemnización". Los primeros apartados dedicados a la tutela de derechos establecían que: "1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los afectados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine. 2. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo. En cambio, en el actual artículo 18 LOPD, tras repetir en su apartado 1 lo que indicaba el 17.1 LORTAD se alude expresamente a los derechos ARCO en su apartado 2: "El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación".

[1135] Si se accede al sitio web de la AEPD, donde se publican las resoluciones por tutela de derechos se puede observar que todos los procedimientos se inician por vulneración de los artículos de la LOPD relativos a los derechos ARCO (principalmente por los artículos 15 y 16 LOPD que se refieren a los derechos de acceso, rectificación y cancelación), http://www.agpd.es, fecha consulta: 23.6.2015. También confirma esta práctica N. BUISÁN GARCÍA, "Artículo 18. Tutela de los derechos", C. LESMES SERRANO (Coord.), VVAA, *La Ley de protección de datos: análisis y comentario de su jurisprudencia*, Lex Nova, Valladolid, 2008, pág. 384.

[1136] Así, la regulación del procedimiento de tutela de derechos se ha incluido en el Capítulo II del Título IX RLOPD bajo la rúbrica "Procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición".

[1137] La AEPD podrá iniciar un procedimiento sancionador si el responsable no atendiera su requerimiento (art. 44.3.i LOPD) o también podrá iniciarlo por impedimento u obstaculización del ejercicio de los derechos ARCO (art. 44.3.e LOPD).

Si bien, el denunciante en un procedimiento sancionador no está legitimado para poder recurrir la resolución de la AEPD, el Tribunal Supremo ha reconocido la legitimación activa al titular de los datos en aquellos procedimientos relacionados con la función de protección del derecho[1138]. Es decir, principalmente se admite esta legitimación en los procedimientos de tutela de derechos, de forma que la decisión de la autoridad pueda ser impugnada en vía jurisdiccional, como cualquier otra decisión de derecho administrativo, de forma que se asegure la protección que reconoce el artículo 53 CE[1139].

2.3. Mecanismos procesales

De algunos estudios realizados a nivel europeo se concluye que, pese a que, en teoría, los Estados miembros han cumplido con la adopción de las vías de recurso que demandaba la Directiva 95/46/CE[1140], éstas no son, en la práctica, todo lo eficaces que debieran[1141]. Destaca el caso del Reino Unido en el que se señalaba la dificultad que tienen los interesados al acceder a la vía judicial[1142].

[1138] STS de 25 de marzo de 2014 (Sala 3ª) (ROJ:STS 1203/2014), FJ 2.

[1139] *Ibídem.*

[1140] Así se concluía en un estudio de las legislaciones de los 27 Estados miembros encargado por la Agencia de Derechos Fundamentales de la Unión Europea (FRA) que se realizó en el año 2009 y dio como resultado que, en las legislaciones de los Estados miembros, en todos los casos, se ha previsto la posibilidad de la vía judicial y prácticamente en todos los casos se ha establecido la reclamación administrativa ante la autoridad de control, excepto en Bélgica. *Data protection in the European Union: the role of national data protection authorities, strengthening the fundamental rights architecture in the EU II, European Union Agency for Fundamental Rights, Publications Office of the European Union, Luxembourg, 2010*, pág. 32. http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf (fecha consulta: 13.8.2014). En Bélgica la autoridad de control (*Commission de la protection de la vie privée*) no es la que impone las sanciones, sino que son los órganos jurisdiccionales los que lo hacen, y, en caso de reclamación por parte de un afectado que estime que se le han vulnerado sus derechos lo que lleva a cabo es un procedimiento de mediación. También puede comunicarlo al *Procureur du Roi* o acudir a los tribunales de primera instancia (art. 32 Ley belga).

[1141] En un estudio contratado por la Comisión Europea publicado en 2010 se establecía que en algunos Estados miembros, especialmente en el Reino Unido, existían obstáculos en la interposición de recursos como el coste, lo que imposibilitaba que los afectados pudieran ejercer este derecho. *Comparative study on different approaches to new privacy challenges, in particular in the Light of technological developments, Contract _r: JLS/2008/C4/011 – 30-CE-0219363/00-28, Final report, LRDP KANTOR Ltd & Centre for Public Reform, European Commission, Directorate General Justice, Freedom and Security, 20 January 2010*, págs. 45 a 46. Asimismo, recuerda la FRA, en un dictamen sobre la reforma y a raíz de otro informe elaborado sobre el rol de las autoridades de protección de datos, que, según jurisprudencia del TEDH, los recursos disponibles deben responder a criterios de disponibilidad, adecuación y efectividad. No es suficiente que el recurso esté disponible teóricamente en virtud de la ley, sino que debe ser efectivo en la práctica. Esta efectividad puede verse truncada por razones ligadas a la complejidad de los procedimientos, su duración o cargas adicionales. *Avis FRA – 2/2012 de l'Agence des droits fondamentaux de l'Union européenne concernant le programme de réforme des règles en matière de protection des données à*

En el ordenamiento jurídico español, ante la vulneración del derecho a la protección de datos, el afectado dispone de diversas vías de distinta naturaleza para poder actuar contra esta vulneración.

Al tratarse de un derecho fundamental, el derecho a la protección de datos goza de la protección del sistema de garantías previsto en nuestro ordenamiento. Este sistema se recoge básicamente en el Capítulo IV del Título I de la Constitución[1143]. Los derechos fundamentales podrán ser invocados por sus titulares ante la vía jurisdiccional

caractère personnel, 1 d'octobre 2012, pág. 30, http://fra.europa.eu/sites/default/files/fra-opinion_2-2012-data-protection_fr.pdf (fecha consulta: 13.8.2014) y *Data protection in the European Union: the role of national data protection authorities, strengthening the fundamental rights architecture in the EU II, op.cit.*.

[1142] Respecto al Reino Unido, en un estudio concreto referido al país, se indica que pese a que se prevea la tutela judicial en caso de que el responsable no atienda el ejercicio de derechos por parte del titular de los datos (Sección 10 Ley inglesa) esto no proporciona una efectiva protección a este titular, ya que los procesos judiciales en el Reino Unido son costosos y, por ello, es raro que en la práctica se opte por esta vía que, según el informe sólo utilizan las celebridades. La Ley inglesa (Sección 42 y siguientes) establece además un procedimiento para atender las solicitudes de cualquier persona respecto a posibles vulneraciones de protección de datos, en consonancia con el artículo 28.4 Directiva 95/46/CE. La autoridad de control primero filtra la petición de forma que debe versar sobre un asunto que tenga cierta entidad, que se hayan cumplido los posibles plazos pertinentes y que la persona ostentara la capacidad de ejercer un derecho de acceso. Después se regula pormenorizadamente el procedimiento, especialmente en lo referente a las salvaguardas establecidas para el responsable: la información que se le puede solicitar, el contenido que debe tener el requerimiento de información que entre otras cosas debe incluir el derecho que tiene el requerido a recurrir, cuando no se puede requerir información (p.ej. cuando la información versa sobre comunicaciones entre un abogado y su cliente, cuando la información revelara la comisión de otra infracción ajena a la ley de protección de datos que le pudiera exponer a otro procedimiento); incluso se establece la posibilidad de que la autoridad cancele el requerimiento de información. Como indica KORFF, el procedimiento que se regula en la ley se percibe hasta casi contrario a la idea de que la autoridad de control lleve a cabo una investigación seria ante las posibles reclamaciones de los interesados. El autor concluye que la autoridad de control inglesa (el ICO) sólo persigue una fracción mínima de las reclamaciones que se interponen y que se trata de una autoridad débil en la persecución del cumplimiento de lo establecido en la ley. D. KORFF, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Country Studies*, A.6-*United Kingdom, op. cit*., págs. 57 a 59.

[1143] Si bien para tener un mapa completo de las garantías hay que acudir a otras partes de la Constitución, como a los Títulos IX y X que se refieren al Tribunal Constitucional y a la reforma constitucional, respectivamente. L. M. DÍEZ-PICAZO, *Sistema de derechos fundamentales, op. cit.*, págs. 69 a 70.

ordinaria[1144] y además también se han establecido dos vías procesales específicas: un procedimiento preferente y sumario y el recurso de amparo ante el TC[1145].

Tras agotar las vías judiciales procedentes, el ciudadano podrá interponer el recurso de amparo ante el TC[1146]. Para ello la materia sobre la que verse el amparo debe ser de especial trascendencia constitucional y debe contarse con la legitimación requerida (arts. 46 a 50 Ley Orgánica 2/1979[1147]).

[1144] DÍEZ-PICAZO establece un catálogo de garantías de los derechos fundamentales en el que diferencia según si éstas lo son frente al legislador o frente a la Administración y el Poder Judicial. Asimismo, dentro de cada una de estas categorías distingue las garantías según si se producen en el plano sustantivo o procesal. Así, dentro de las garantías frente a la Administración y el Poder Judicial, en el plano procesal, se encuentran: el control judicial de la Administración (art. 106 CE) y la existencia de un sistema de recursos contra resoluciones judiciales. La posibilidad de que un particular pueda invocar sus derechos ante cualquier juez o tribunal y en cualquier tipo de proceso es consecuencia, según el autor, de la aplicabilidad directa de la Constitución, según se desprende del artículo 9 CE y de la interpretación *a contrario* del inciso final del art. 53.3 CE. L. M. DÍEZ-PICAZO, *Sistema de derechos fundamentales, op. cit.*, págs. 70 a 75.

[1145] Así, el artículo 53.2 CE prevé que "cualquier ciudadano podrá recabar la tutela de las libertades y derechos reconocidos en el artículo 14 y la Sección primera del Capítulo segundo ante los Tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional". Este procedimiento preferente y sumario de protección de los derechos fundamentales se ha establecido en los órdenes administrativo, laboral y militar, mientras que no existe en materia civil y penal. En lo que respecta al ordenamiento administrativo, es la Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contencioso-administrativa (BOE núm. 167 de 14.7.1998) la que establece, entre los procedimientos especiales, la regulación del procedimiento para la protección de los derechos fundamentales en sus artículos 114 a 122bis. En el ordenamiento laboral es la Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social (BOE núm. 245 de 11.10.2011) la que regula un procedimiento preferente en sus artículos 177 a 184 para la protección de los derechos fundamentales. L. M. DÍEZ-PICAZO, *Sistema de derechos fundamentales, op. cit.*, págs. 75 a 79. Hay que señalar, no obstante, que en el ordenamiento civil la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (BOE núm. 7 de 8.1.2000), en su artículo 249.1.2º, señala el carácter preferente y la necesaria actuación como parte del Ministerio Fiscal en la tramitación de juicios en los que se solicite la tutela judicial civil de derechos fundamentales. Por tanto, MORENILLA considera que, pese a tratarse de un procedimiento ordinario y no especial como el que establecen las leyes administrativa y laboral, cumpliría con el artículo 53.2 CE. P. MORENILLA ALLARD, "Tutela procesal civil de los derechos fundamentales", V. GIMENO SENDRA, P. MORENILLA ALLARD, *Los procesos de amparo. Civil, penal, administrativo, laboral, constitucional y europeo*, *op. cit.*, págs. 20 a 21.

[1146] El derecho a la protección de datos estaría entre los derechos que admiten la interposición del recurso de amparo. Artículo 41 Ley Orgánica 2/1979, de 3 de octubre, del Tribunal Constitucional (BOE núm. 239, de 5.10.1979).

[1147] Desde la importante reforma que se realizó mediante la Ley Orgánica 6/2007, de 24 de mayo, por la que se modifica la Ley Orgánica 2/1979, de 3 de octubre, del Tribunal Constitucional (BOE núm. 125 de 25.5.2007) se introdujo esta regla de admisión del recurso de amparo que tuvo como finalidad evitar el colapso ante el gran volumen de recursos presentados. El TC entrará al fondo del asunto si se justifica por la importancia para interpretar la Constitución, para su aplicación o para su general eficacia y para la determinación del contenido y alcance de los derechos fundamentales (art. 50.1.b Ley Orgánica 2/1979). Estos criterios que determinan que existe trascendencia constitucional configuran el recurso de amparo como una garantía extraordinaria. La reforma se complementó con la modificación del incidente de nulidad de actuaciones (art. 241 Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, BOE de 2.7.1985) de forma que se reforzó la jurisdicción ordinaria como garante habitual de los derechos fundamentales, al ampliarse el ámbito de este incidente a la vulneración de cualquier derecho fundamental y no sólo para los supuestos de indefensión o incongruencia, como estaba antes de la reforma. M. CARRILLO, "La objetivación del recurso de amparo: una nueva vía de garantía jurisdiccional de los derechos", M. CARRILLO, R.

Respecto a la legitimación para interponer un recurso de amparo el TC admitió la misma respecto a una entidad bancaria, en calidad de responsable del fichero. La entidad bancaria interpuso un recurso de amparo por entender vulnerado su derecho a la tutela judicial efectiva (art. 24.1 CE) por un auto judicial que le obligaba a ceder datos personales de algunos de sus clientes a una asociación de defensa de los derechos de los consumidores, en el marco de unas diligencias preliminares[1148].

Así, el TC, en contra de dicha asociación y el Ministerio Fiscal, entendió que el banco tenía legitimación activa ya que se cumplían los requisitos exigidos para ello: que la entidad bancaria había sido parte en el proceso judicial y que invocaba un interés legítimo[1149]. Al valorar si concurría interés legítimo en la entidad bancaria, el TC analizó si ésta podía esgrimir la vulneración de su derecho a la tutela judicial efectiva en conexión con el derecho a la protección de datos de sus clientes.

El TC entendió que el banco no esgrimía derechos ajenos, ya que entonces no cabría admitirse la legitimación, sino que lo que hacía era cuestionar que el órgano judicial no ponderó suficientemente la afectación que suponía la cesión de datos para los derechos fundamentales de sus clientes. Y ello era así porque la entidad bancaria era la responsable de los ficheros en los que se contenían esos datos y, por lo tanto, era responsable de su adecuado tratamiento, uso y custodia, lo que hacía que debiera admitirse la legitimación y finalmente incluso se le otorgara el amparo reconociéndole su derecho a la tutela judicial efectiva en conexión con el derecho a la protección de datos[1150].

ROMBOLI, *La reforma del recurso de amparo*, Fundación Coloquio Jurídico Europeo, Madrid, 2012, págs. 53, 59.

[1148] STC 96/2012, de 7 de mayo de 2012.

[1149] Ambos requisitos los extrae el TC de los artículos 162.1 b) CE y 46.1 b) Ley Orgánica 2/1979, de 3 de octubre, del Tribunal Constitucional. El TC entiende que concurre interés legítimo en todo aquel cuyo círculo jurídico pueda resultar afectado por la violación de un derecho fundamental, aunque dicha vulneración no se haya producido directamente en su contra y sin que ello signifique que en el recurso de amparo exista la acción pública. STC 96/2012, de 7 de mayo de 2012, FJ 2.

[1150] STC 96/2012, de 7 de mayo de 2012, FJ 2. En este sentido, el TC también se pronunció en otro recurso de amparo, posterior al mencionado, interpuesto por algunos de los clientes de la entidad bancaria, ya que el órgano judicial que había dictado el auto controvertido les había denegado la personación que habían solicitado. El TC les otorga el amparo por vulneración de su derecho a la tutela judicial efectiva, ya que entiende el tribunal que no había duda que en el procedimiento se había planteado una cuestión que afectaba directamente a los clientes ya que eran sus datos personales los que la entidad bancaria debía ceder a la asociación y ello podía conllevar una lesión de su derecho a la protección de datos. STC 219/2012, de 26 de noviembre de 2012.

En caso de que no se admitiera el recurso de amparo, no se cumplieran los requisitos establecidos en la ley para interponerlo o no se otorgara el mismo, hay que recordar que quedará también la posibilidad de acudir al TEDH.

Hay que tener en cuenta que, cuando lo que se solicite sea el derecho de indemnización (art. 19 LOPD), no podrá acudirse a las autoridades de control[1151] ni es exigible una actuación previa de estas autoridades[1152]. El titular de los datos, en estos casos acudirá a la jurisdicción ordinaria, ya sea la civil, penal o la contencioso-administrativa si se trata de ficheros de titularidad pública (art. 19 apdos. 2 y 3 LOPD).

2.4. Responsabilidad

2.4.1. Responsabilidad civil

a. Diferencias entre las leyes nacionales de los Estados miembros de la Unión Europea y el artículo 23 Directiva 95/46/CE

En lo que se refiere a las divergencias entre el artículo 23 Directiva 95/46/CE y las leyes de los Estados miembros de la UE, cabe señalar las Leyes danesa e inglesa que exoneran al responsable si, pese a que hubiera actuado con la diligencia exigible, no hubiera podido evitar el daño[1153]. La Ley griega no determina el sujeto que debe indemnizar, sino que se limita a especificar que debe hacerlo aquél que, al vulnerar la ley cause un daño material o moral[1154].

[1151] J. PUYOL MONTERO, "Derecho a indemnización", A. TRONCOSO REIGADA (Dir.). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.,* pág. 1.265.
[1152] SAP Barcelona de 17 de julio de 2014 (Sección 16) (ROJ: SAP B 8246/2014), FFJJ 7,17.
[1153] Así la Ley danesa especifica que el responsable no deberá indemnizar el daño si éste no se hubiera podido evitar a pesar de haber actuado con la máxima diligencia (art. 69 Ley danesa). Asimismo, la Ley inglesa establece que el destinatario de la reclamación puede argumentar que tuvo el cuidado que las circunstancias razonablemente exigían para cumplir el requerimiento controvertido (Sección 13 Ley inglesa). Además, se limita la indemnización en lo que se refiere al daño moral que sólo podrá reclamarse si el sujeto ha sufrido también daños materiales, a no ser que el daño moral fuera resultado de la vulneración de la ley en lo relativo a tratamientos de datos con fines periodísticos, artísticos o literarios.
[1154] Por tanto, otra característica, es que considera incluido tanto el daño material como el moral (art. 23 Ley griega).

En un estudio realizado el año 2010, se detectó que en algunos Estados miembros no era posible la reclamación de indemnización por daños en el caso de vulneración del derecho a la protección de datos. Esto se achacaba a diversos factores que se combinaban como la carga de la prueba, las dificultades en la cuantificación de los daños y la falta de apoyo de las autoridades de control más centradas en actividades promocionales.[1155]. En algunos informes se sugería como posible solución que las mismas autoridades de control pudieran encargarse de otorgar indemnizaciones[1156].

El artículo 23 Directiva 95/46/CE encuentra su reflejo en el ordenamiento español en el artículo 19 LOPD que establece el derecho a indemnización que tienen los interesados. No obstante, se aprecian algunas diferencias en ambos preceptos. Hay que destacar sobre todo el hecho de que la LOPD amplíe los sujetos responsables respecto a la Directiva 95/46/CE, ya que además del responsable contempla la responsabilidad del encargado del tratamiento[1157]. Otra diferencia a subrayar es que la LOPD no incluye causas de exoneración de responsabilidad que sí contempla la Directiva 95/46/CE, aunque en la parte de los Considerandos.

La Directiva 95/46/CE establece como factor que origina el derecho a la indemnización que se produzca un perjuicio, como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales. En cambio, este factor en la LOPD es el incumplimiento de la propia LOPD. Por último, la LOPD realiza una distinción entre ficheros de titularidad pública y ficheros de titularidad privada. Hay que tener en cuenta que la Directiva 95/46/CE no distingue entre estos dos tipos de tratamientos. De esta forma, el artículo 19.2 LOPD remite a la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas en el caso de ficheros de

[1155] Los países señalados eran Finlandia, Irlanda, Holanda, Reino Unido, Chipre, Malta, Polonia, Letonia, Estonia y Suecia en lo referido a la indemnización proveniente de entidades privadas. *Data protection in the European Union: the role of national data protection authorities, strengthening the fundamental rights architecture in the EU II, op.cit.*, pág. 43.

[1156] Así lo sugería la misma FRA que examinó los mecanismos de recurso en el campo de la protección de datos y los resultados fueron que las víctimas de violaciones de este derecho eran reticentes a acceder a la justicia para dirigirse contra los responsables. La FRA proponía que las autoridades de control pudieran también reparar, es decir, otorgar indemnizaciones, de forma que se facilitara la eficacia de este mecanismo. *Avis FRA – 2/2012 de l'Agence des droits fondamentaux de l'Union européenne concernant le programme de réforme des règles en matière de protection des données à caractère personnel, op. cit.,* pág. 30.

[1157] GRIMALT SERVERA aludía a esta limitación relativa al sujeto agresor, aunque el autor sólo se refería al responsable, ya que en el momento en el que realizó su estudio sobre la responsabilidad civil estaba vigente la LORTAD que no establecía la figura del encargado del tratamiento. P. GRIMALT SERVERA, *La responsabilidad civil en el tratamiento automatizado de datos personales, op.cit.* pág. 4.

titularidad pública y el artículo 19.3 LOPD indica que, en el caso de ficheros de titularidad privada, debe acudirse a la jurisdicción ordinaria.

b. El derecho a indemnización de la Ley Orgánica 15/1999

i. La formulación y naturaleza de la responsabilidad

El régimen de responsabilidad en la LOPD se establece como un derecho de los titulares de los datos a ser indemnizados cuando sufran daño o lesión en sus bienes o derechos, como consecuencia del incumplimiento de lo dispuesto en la LOPD por el responsable o el encargado del tratamiento (art. 19 LOPD). Esta formulación desde una perspectiva positiva de quien detenta el derecho a ser indemnizado está en consonancia con el enunciado de la Directiva 95/46/CE.

Como se ha indicado, el factor detonante del derecho a la indemnización es el incumplimiento de la LOPD, por lo que los supuestos que generarán responsabilidad serán los establecidos en esta ley de acuerdo con un sistema típico de responsabilidad[1158]. ¿Qué quiere decir incumplimiento? ¿Debe considerarse que se refiere a cualquier incumplimiento de la LOPD o sólo a aquél que aparezca tipificado como infracción en el catálogo del régimen sancionador (art. 44 LOPD)?

La limitación de los incumplimientos generadores de derecho a indemnización a aquellos que suponen infracciones en el régimen sancionador no parece acorde con las naturalezas diferentes de la responsabilidad civil y del régimen sancionador[1159]. Así lo ha confirmado el Tribunal Supremo en un asunto en el que los demandados, empresas gestoras de un canal de televisión, habían argumentado que sin resolución de la AEPD

[1158] L. DÍEZ-PICAZO, *Fundamentos del derecho civil patrimonial. V La responsabilidad civil extracontractual*, *op. cit.*, pág. 304. J.M. BUSTO LAGO, "La responsabilidad de los responsables de ficheros de datos personales y de los encargados de su tratamiento", *Revista Aranzadi Civil-Mercantil, op. cit.*, pág. 16.

[1159] PUYOL MONTERO entiende que cualquier infracción de lo establecido en la LOPD puede dar derecho a indemnización. J. PUYOL MONTERO, "Derecho a indemnización", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, pág. 1.268. No obstante, hay que mencionar una sentencia del Tribunal Supremo que, aunque en *obiter dicta*, en un asunto en el que considera que no se puede aplicar la LOPD por no entrar en su ámbito de aplicación, especifica que no se incurrió en ninguna infracción de las previstas en el catálogo del régimen sancionador (art. 44 LOPD) y, por tanto, no podía generarse indemnización (art. 19 LOPD). STS de 17 de septiembre de 2014 (Sala 1ª) (ROJ: STS 3524/2014), FJ 9.

que hubiera declarado existencia de infracción de la LOPD, los tribunales civiles no podían establecer una indemnización[1160].

El Alto tribunal recuerda que, así como los tribunales del orden civil carecen de potestad sancionadora y tampoco pueden ejercer control jurisdiccional de las decisiones de la AEPD, sí que ostentan jurisdicción para decidir sobre la procedencia o no de condenar a los infractores a indemnizar por los daños ocasionados por incumplimiento de la LOPD, siempre que se trate de ficheros de titularidad privada[1161]. Por tanto, los tribunales civiles para estimar si cabe o no la indemnización deben, previamente, decidir sobre la realidad de las infracciones[1162]. Esta libre apreciación entiendo que no debe constreñirse al catálogo de infracciones que se ha diseñado para cumplir con la finalidad punitiva del derecho administrativo sancionador.

Aún es más contundente el Tribunal Supremo, cuando considera responsable a un titular de un fichero común de morosos, en contra del juez de primera instancia, que había aplicado una disposición reglamentaria (art. 44.3.1.a RLOPD)[1163]. Esta disposición establece que, si un afectado dirige una solicitud de ejercicio de derechos al titular del fichero común, éste debe trasladar la solicitud a la entidad que le ha facilitado los datos para que sea ésta la que resuelva.

El Tribunal Supremo rechaza la aplicación de esta previsión reglamentaria, al entender que en aplicación de normas superiores como son la misma LOPD, la Carta UE, la Directiva 95/46/CE o el Convenio 108, el titular del fichero común no podía limitarse a trasladar la solicitud y seguir las indicaciones de la entidad que facilitó los datos, sino que debía realizar su propia valoración del derecho de cancelación[1164].

Además, en esta sentencia, el Tribunal Supremo se refiere a la anulación que había llevado a cabo este mismo tribunal de otra disposición reglamentaria (art. 38.2 RLOPD) que preveía que no se pudieran incluir datos en el fichero común si existía un principio de

[1160] Tras la sentencia de primera instancia que los condenaba a indemnizar por haber entendido el tribunal que habían incumplido la LOPD, los demandados obtuvieron resolución favorable de la AEPD. STS de 30 de marzo de 2011 (Sala 1ª) (ROJ: STS 2227/2011), FJ 2.
[1161] STS de 30 de marzo de 2011 (Sala 1ª) (ROJ: STS 2227/2011), FJ 3.
[1162] *Ibídem*.
[1163] STS de 21 de mayo de 2014 (Sala 1ª) (ROJ: STS 267/2014).
[1164] *Ibídem*, FJ 8.

prueba que contradijera los requisitos que se exigían para esa inclusión[1165]. El Alto Tribunal considera que esta anulación, que también apoyaría la tesis del juzgador de primera instancia, se realizó en respuesta a exigencias propias del derecho administrativo sancionador, pero no debe tenerse en cuenta a efectos de una reclamación de responsabilidad civil. Por tanto, con este pronunciamiento se manifiestan claramente las diferencias de criterios según si nos hallamos en el derecho administrativo sancionador o en el derecho civil y sirve para mostrar los diferentes resultados que pueden obtenerse dependiendo de la vía por la que se opte[1166].

El hecho de que los supuestos que generan responsabilidad estén contemplados en la ley ¿debe considerar que estamos ante una responsabilidad extracontractual? ¿O también podríamos hallarnos ante supuestos de responsabilidad contractual? La respuesta no carece de trascendencia en la práctica, ya que de ella dependen cuestiones tan importantes como el plazo de prescripción de las acciones que pueden interponerse en un caso o en el otro[1167]. Hay que entender que, aunque los supuestos estén establecidos en la ley, ello no impedirá que podamos hallarnos ante casos de responsabilidad contractual o extracontractual[1168]. De hecho, la mayoría de autores consideran que la responsabilidad

[1165] Requisitos que se establecen en el artículo 38.1 RLOPD y que consisten en: que la deuda sea cierta, vencida, exigible, impagada y respecto a la que no se hayan entablado reclamación judicial, arbitral o administrativa o si son servicios financieros, no se haya planteado reclamación en los términos del Real Decreto 303/2004, de 20 de febrero; que no hayan transcurrido seis años desde que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto si fuera de vencimiento periódico; que se haya realizado requerimiento previo de pago. El artículo 38.2 RLOPD fue anulado por la STS de 15 de julio de 2010 (Sala 3ª) (ROJ: STS 4050/2010).

[1166] Por tanto, no se lograría la coherencia entre las diferentes decisiones judiciales a la que aludía D. ORDÓÑEZ SOLÍS, *Privacidad y protección judicial de los datos personales*, *op. cit.*, págs. 215 a 216. Es importante a la hora de establecer una estrategia jurídica tener en cuenta el objetivo que se persigue y la vía que puede ser más eficaz para obtenerlo.

[1167] Las acciones personales que no tienen señalado plazo especial prescriben a los quince años (art. 1.964 Cc). En este grupo se consideran incluidas las acciones para exigir la responsabilidad contractual. La acción para exigir la responsabilidad extracontractual prescribe por el transcurso de un año (art. 1968.2º Cc). En el Código civil de Cataluña, se establece el plazo de diez años para las pretensiones de cualquier clase y prescriben a los tres años, entre otras, las pretensiones derivadas de responsabilidad extracontractual (arts. 121-20 y 121-21 Ley 29/2002, de 30 de diciembre, primera ley del Código civil de Cataluña (DOGC núm. 3798 de 13.1.2003). Hay que tener en cuenta que, cuando la obligación deba sujetarse al derecho civil catalán, el Tribunal Superior de Justicia de Cataluña ha estimado que deben aplicarse los plazos de prescripción del Código civil de Cataluña, aunque la institución civil no haya sido plenamente desarrollada por esta norma, en virtud de la aplicación del código catalán como norma de derecho común. Ver sentencia del Tribunal Superior de Justicia de Cataluña de 12 de septiembre de 2011 (Sala de lo Civil y lo Penal) (ROJ: STSJ CAT 9602/2011), FFJJ 2,6 y J.M. ABRIL CAMPOY, "La prescripción en el derecho civil de Cataluña: ¿es aplicable la normativa catalana solamente cuando existe regulación propia de la pretensión que prescribe?", *InDret* 2/2011 abril, Barcelona, 2011, http://www.indret.com/pdf/817_es.pdf, (fecha consulta: 2.9.2015), pág. 27.

[1168] La responsabilidad civil se considera que puede venir establecida por un mandato legal o puede derivar del incumplimiento de lo pactado (contractual) o puede originarse por haber producido un daño sin existir

de la LOPD es una responsabilidad eminentemente extracontractual, aunque también se admite que puede ser contractual[1169].

La responsabilidad contractual es la que deriva del incumplimiento de lo pactado entre el causante del daño y la víctima del mismo[1170]. Algunos preceptos de la LOPD pueden originar la inclusión de pactos en los contratos suscritos entre el responsable y el titular de los datos. Así, si el responsable debe suscribir un contrato con el titular de los datos podría incluir en el mismo, el texto que cumpla con el deber de información que tiene respecto al titular (art. 5 LOPD). De esta forma, el contrato podría constituir la prueba de que ha cumplido con este deber. Si se ocasionaran daños al titular de los datos como consecuencia de que el texto incluido en el contrato no cumpliera con lo previsto en la LOPD, podría considerarse que estamos ante una responsabilidad contractual, ya que su fuente sería el incumplimiento del contrato.

No obstante, el factor esencial que origina el derecho de indemnización es el incumplimiento de la LOPD, independientemente de que también, al mismo tiempo, se

---

ninguna relación previa (o porque se produce fuera de su ámbito) entre quien produce el daño y la víctima del mismo (extracontractual). No obstante, DE ÁNGEL YAGÜEZ considera que cuando las leyes establecen deberes a los sujetos, esto no impide que pueda hablarse de responsabilidad extracontractual cuando estos sujetos incumplan estos deberes. La razón es que estas reglas contenidas en las leyes pretenden proteger a cualquiera que sufra daños ocasionados por su incumplimiento y no a un concreto individuo perjudicado. De esta forma no existiría relación previa (y, por tanto, responsabilidad contractual) en la responsabilidad legal entre el sujeto causante del daño y la víctima del mismo. R. DE ÁNGEL YAGÜEZ, "La responsabilidad civil. Cuestiones previas de delimitación", I. SIERRA GIL DE LA CUESTA, R. DE ÁNGEL YAGÜEZ [et al.] (Coord.), VVAA, *Tratado de responsabilidad civil*, *op. cit.*, págs. 9, 12.

[1169] Así lo entienden P. GRIMALT SERVERA, *La responsabilidad civil en el tratamiento automatizado de datos personales, op.cit.,* pág. 225 (que se pronuncia respecto a la LORTAD); J.M. BUSTO LAGO, "La responsabilidad de los responsables de ficheros de datos personales y de los encargados de su tratamiento", *Revista Aranzadi Civil-Mercantil, op. cit.*, pág. 15; M. HEREDERO HIGUERAS. *La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (Comentarios y textos), op. cit.,* pág. 140 (también referido a la LORTAD); J. PUYOL MONTERO, "Derecho a indemnización", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.,* pág. 1.268. Califica esta responsabilidad de extracontractual respecto a la LORTAD: A. ORTÍ VALLEJO, *Derecho a la intimidad e informática (Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada),* Comares, Granada, 1994, pág. 170.

[1170] La jurisprudencia del Tribunal Supremo ha determinado que, aunque el daño aparezca vinculado a la existencia de una relación jurídica previa, si no acontece dentro de la rigurosa órbita de lo pactado y como preciso desarrollo del contenido negocial, entonces el hecho dañoso es violación de una obligación contractual y, al mismo tiempo del deber de no dañar a otro, por lo que hay una yuxtaposición de responsabilidad, contractual y extracontractual. Como indica ASÚA GONZÁLEZ, no queda claro el criterio utilizado por el Tribunal Supremo para delimitar la zona en la que convergen la responsabilidad contractual y la extracontractual. C.I. ASÚA GONZÁLEZ, "La responsabilidad(I)", L. PUIG I FERRIOL, M.C. GETE-ALONSO Y CALERA, J. GIL RODRÍGUEZ, J.J. HUALDE SÁNCHEZ, *Manual de derecho civil II, derecho de obligaciones, responsabilidad civil, teoría general del contrato*, Marcial Pons, Madrid, Barcelona, 1998, pág. 457 a 460.

incumpla una obligación contractual. Esto supondrá que el interesado disponga, ante un mismo hecho, de dos pretensiones resarcitorias distintas, una fundamentada en las normas de responsabilidad contractual y otra en la responsabilidad extracontractual[1171].

Otra cuestión que cabe plantear es el supuesto en el que el responsable se obligue mediante contrato a ir más allá de lo previsto en la ley. En estos casos, no podría reclamarse indemnización en el ámbito del artículo 19 LOPD, sino que debería acudirse a la regulación del Código civil en materia de responsabilidad contractual.

En este sentido también se puede añadir el supuesto en el que el responsable se adhiera a un código de conducta o código tipo. En ambos casos, ante el incumplimiento de este código de conducta ¿se podrá entender que podría nacer el derecho a indemnización previsto en la LOPD?

A este respecto, hay que tener en cuenta la incorporación en la LOPD de una regulación de este instrumento (art. 32 LOPD y 71 ss. RLOPD)[1172]. Consecuentemente, si el incumplimiento del código conlleva un incumplimiento de esta regulación específica, entiendo que puede generarse la obligación de indemnizar del artículo 19 LOPD. Lo mismo sucederá si se incumple alguna disposición del código tipo que reproduce una obligación establecida en la legislación de protección de datos. Ahora bien, las obligaciones que vayan más allá de estos supuestos no podrían entrar dentro del ámbito del artículo 19 LOPD[1173]. De nuevo, habría que acudir a lo establecido en el Código civil.

Sin embargo, los códigos tipo podrán incorporar sus propios procedimientos para determinar medidas reparadoras si se produce algún perjuicio a los afectados como consecuencia del incumplimiento del código (art. 75.3 RLOPD). Estas medidas podrán establecerse "sin perjuicio de lo dispuesto en el artículo 19", lo que parece indicarse para clarificar que, aunque se adopten, debe respetarse la competencia atribuida a otros

[1171] C.I. ASÚA GONZÁLEZ, "La responsabilidad(I)", L. PUIG I FERRIOL, M.C. GETE-ALONSO Y CALERA, J. GIL RODRÍGUEZ, J.J. HUALDE SÁNCHEZ, *Manual de derecho civil II, derecho de obligaciones, responsabilidad civil, teoría general del contrato, op. cit.*, pág. 457.
[1172] Ver Capítulo VI.
[1173] P. GRIMALT SERVERA, *La responsabilidad civil en el tratamiento automatizado de datos personales, op.cit.*, págs. 224 a 225.

órganos en virtud del artículo 19 LOPD para dirimir si hay obligación de indemnizar[1174]. La incorporación de estas medidas no puede suponer que se arrogue esa competencia en todos los casos susceptibles de generar daño a un órgano establecido por el código tipo.

La responsabilidad que deriva de lo establecido en el código tipo se puede calificar de contractual al entender que se trata de un contrato a favor de terceros[1175]. De esta forma, la utilización de códigos tipo tendría importantes incentivos, como pueden ser la aplicación del plazo de prescripción de la responsabilidad contractual.

ii. Delimitación con otros regímenes de responsabilidad civil

(1) Delimitación con el régimen del Código civil

El régimen de responsabilidad que establece la LOPD ¿es un régimen especial? ¿Contiene una regulación específica de la responsabilidad, frente al régimen general del Código civil o frente a otras regulaciones especiales como la de los derechos de la personalidad que se incluye en la LO 1/1982?[1176]

Esta cuestión entiendo que se suscita respecto a la responsabilidad en materia de ficheros de titularidad privada, ya que, como se ha comentado anteriormente, en el caso de ficheros de titularidad pública se produce una remisión a la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas.

[1174] J. RUBÍ NAVARRETE, "Códigos tipo", R. MARTÍNEZ MARTÍNEZ (Coord.). *Protección de datos: comentarios a la LOPD y su reglamento de desarrollo, op. cit.*, pág. 193.

[1175] Si bien GRIMALT SERVERA argumenta que pueden defenderse ambas posturas, la de que se considere responsabilidad contractual o la que defienda el carácter extracontractual, indica que el carácter contractual vendría recogido en el artículo 1.257 Cc: "si el contrato contuviere alguna estipulación a favor de un tercero, éste podrá exigir su cumplimiento, siempre que hubiese hecho saber al obligado antes de que haya sido aquélla revocada". P. GRIMALT SERVERA, *La responsabilidad civil en el tratamiento automatizado de datos personales, op.cit.* pág. 224.

[1176] Aunque no deba guiar la respuesta a estas preguntas, lo cierto es que en los manuales de derecho civil no se incluye esta disposición de la LOPD entre las legislaciones especiales que contienen disposiciones sobre responsabilidad civil, entre las que se suelen citar las leyes de navegación aérea, sobre la responsabilidad civil y seguro en la circulación de vehículos a motor, de la energía nuclear, de caza o de defensa de consumidores y usuarios. Baste citar a C.I. ASÚA GONZÁLEZ, "La responsabilidad(I)", L. PUIG I FERRIOL, M.C. GETE-ALONSO Y CALERA, J. GIL RODRÍGUEZ, J.J. HUALDE SÁNCHEZ, *Manual de derecho civil II, derecho de obligaciones, responsabilidad civil, teoría general del contrato, op. cit.*, págs. 456 a 457. Como excepción, se menciona la LOPD como ley en materia de responsabilidad civil posterior al Cc en: R. DE ÁNGEL YAGÜEZ, "La responsabilidad civil. Cuestiones previas de delimitación", I. SIERRA GIL DE LA CUESTA, R. DE ÁNGEL YAGÜEZ [et al.] (Coord.), VVAA, *Tratado de responsabilidad civil, Tomo I, op. cit.*, pág. 110.

La delimitación del régimen de responsabilidad de la LOPD frente al del Código civil tendrá importancia para determinar especialmente los títulos de imputación cuando estamos ante un supuesto de responsabilidad extracontractual. De esta forma, la diferencia esencial entre ambas regulaciones es que, mientras que el artículo 19 LOPD exige para generar esta responsabilidad que exista un incumplimiento de la ley por parte del responsable o el encargado, el Código civil establece la acción u omisión en la que intervenga culpa o negligencia (art. 1.902 Cc)[1177]. Nos acercaremos a esta cuestión más adelante.

Sin embargo, parece lógico entender que, si el legislador hubiera querido aplicar, sin más el régimen del Código civil se hubiera remitido a esta regulación, de la misma manera que respecto a los ficheros de titularidad pública se ha remitido a la regulación específica de responsabilidad en este sector. Por tanto, hay que considerar que estamos ante una regulación específica cuya característica principal es la limitación de los supuestos que generan la obligación de indemnizar a lo establecido en la LOPD[1178].

Ahora bien, en la medida en que la regulación de la LOPD sea incompleta entiendo que deberá suplirse con lo que establece el Código civil (*ex* 1.090 Cc y en general art. 4.3 Cc) o la regulación autonómica aplicable[1179].

[1177] Hay que recordar los elementos que tradicionalmente conforman la responsabilidad civil extracontractual: a) un comportamiento o conducta; b) que este comportamiento haya provocado un daño; c) que entre ambos exista una relación de causalidad; d) en el ámbito de la responsabilidad subjetiva, que intervenga a modo de criterio de imputación, la culpa. C.I. ASÚA GONZÁLEZ, "La responsabilidad(I)", L. PUIG I FERRIOL, M.C. GETE-ALONSO Y CALERA, J. GIL RODRÍGUEZ, J.J. HUALDE SÁNCHEZ, *Manual de derecho civil II, derecho de obligaciones, responsabilidad civil, teoría general del contrato, op. cit.*, pág. 462.

[1178] Contradice esta postura la Audiencia Provincial de Madrid que en un asunto en el que considera que se ha infringido el artículo 29 LOPD estima el recurso de apelación y considera que cabe la condena a indemnización. Sin embargo, no menciona el artículo 19 LOPD, sino que fundamenta esta obligación en virtud de la responsabilidad civil extracontractual del artículo 1902 Cc. SAP Madrid de 31 de marzo de 2006 (Sección 11) (ROJ: SAP M 4152/2006), FJ 2,3. Asimismo, consideran directamente aplicable la regulación del Código civil en materia de responsabilidad extracontractual T. FREIXES, A. GALLARDO, X. VALLVÉ, *FRANET, Contractor Ad hoc Information Report, Data protection: redress mechanisms and their use, Spain*, Movimiento por la Paz (MPDL), Gabinet d'Estudis Socials (GES), Instituto Europeo de Derecho (IED), 2012, pág. 4.

[1179] Así lo entendió también P. GRIMALT SERVERA, *La responsabilidad civil en el tratamiento automatizado de datos personales, op.cit.* pág. 33 (referido a la LORTAD). Entiende que se aplica directamente la regulación del Cc: M. HEREDERO HIGUERAS. *La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (Comentarios y textos), op. cit.*, pág. 140 (también referido a la LORTAD). Completa la regulación del artículo 19 LOPD con lo que establece el artículo 1902 Cc: M.R. LLÁCER MATACÁS, *La autorización al tratamiento de información personal en la contratación de bienes y servicios. La privacidad, entre el estatuto del*

(2) Delimitación con el régimen de la Ley Orgánica 1/1982

Los derechos de la personalidad, considerados derechos subjetivos absolutos[1180], siempre han gozado tradicionalmente de una protección clara por parte del derecho civil y se ha considerado que la lesión de los mismos debía protegerse con el régimen de responsabilidad extracontractual. Por ello, incluso se incluyó una regulación específica en el artículo 9 LO 1/1982, ley que protege los derechos al honor, a la intimidad personal y familiar y a la propia imagen. Este precepto recoge la necesidad de que exista una tutela judicial frente a intromisiones ilegítimas de estos derechos. Entre las medidas que establece esta norma para asegurar esta tutela judicial está la indemnización de los daños y perjuicios causados.

Una cuestión que se ha planteado es si este precepto debe aplicarse al derecho a la protección de datos, por su conexión con el derecho a la intimidad[1181]. Entiendo, no obstante, que si la LOPD incluye una disposición especifica relativa al derecho a la indemnización y además dispone una regulación autónoma del derecho a la protección de

responsable y la fragilidad del consentimiento, op. cit., pág. 121. ORTÍ VALLEJO entendió que la previsión que contemplaba el artículo 17.3 LORTAD era un régimen especial, excepto respecto a la obligación de secreto (art. 10 LORTAD) y la relativa a la utilización de los datos para finalidad distinta (art. 27.1 en relación al 4.2 LORTAD) en las que consideró que regía el sistema del Cc y respondía el infractor salvo que se diera un caso de responsabilidad el art. 1903 Cc. ORTÍ VALLEJO realizaba esta diferenciación porque en estas disposiciones se generaban obligaciones para sujetos diferentes del responsable. Como la LORTAD sólo preveía la obligación de indemnización a cargo del responsable del fichero, este autor entendió que, ante el incumplimiento de estas obligaciones por parte de estos otros sujetos, debería aplicarse el régimen del Cc. A. ORTÍ VALLEJO, *Derecho a la intimidad e informática (Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada)*, *op. cit.*, pág. 170.

[1180] L. DÍEZ-PICAZO, *Fundamentos del derecho civil patrimonial. V La responsabilidad civil extracontractual, op. cit.*, pág. 297.

[1181] GRIMALT SERVERA estimaba que el derecho a la protección de datos estaba ligado al de la intimidad y, por tanto, que la LO 1/1982 era de aplicación supletoria a la LORTAD. Esta interpretación la recogía en el año 1999, cuando aún no se había producido un reconocimiento claro del carácter de derecho autónomo del derecho a la protección de datos. P. GRIMALT SERVERA, *La responsabilidad civil en el tratamiento automatizado de datos personales, op.cit.*, págs. 31 a 33. Sin embargo, recientemente ha mantenido esta aplicación especial de la LORTAD. GRIMALT SERVERA entiende que los daños ocasionados al derecho de protección de datos generalmente no son relevantes a efectos de indemnización civil si no suponen al mismo tiempo daños a los derechos de intimidad, honor o propia imagen. Y en caso de que los daños afecten a estos derechos debe aplicarse la LO 1/82, ley especial. P. GRIMALT SERVERA, "La necesaria reconducción del régimen jurídico de la protección de los datos personales desde la perspectiva de los conflictos y solapamientos con otros derechos y libertades en internet", VALERO TORRIJOS, J. (Coord), VVAA, *La protección de los datos personales en internet ante la innovación tecnológica. Riesgos, amenazas y respuestas desde la perspectiva jurídica*, *op. cit.*, pág. 66.

datos, no cabría en principio aplicar otra disposición que se refiere a otros derechos diferenciados como son el honor, la intimidad y la imagen[1182].

El hecho de aplicar la regulación contenida en la LO 1/1982 tendría importantes consecuencias, ya que incluye características específicas, como un plazo más amplio para interponer la acción o la presunción de existencia de perjuicio ante una intromisión ilegítima en los derechos que protege. Otra cuestión es que debido a la conexión de los derechos se puedan utilizar algunos criterios a efectos interpretativos, especialmente en la valoración de los daños[1183].

Hay que resaltar la escasa alusión al derecho a la protección de datos en las demandas civiles de solicitud de indemnización cuando, en ocasiones está claro que este derecho ha sido vulnerado. Estas demandas se suelen centrar en los derechos clásicos de la personalidad: intimidad, honor y propia imagen. El reconocimiento relativamente reciente de este derecho como tal y la posibilidad de elegir la vía administrativa que se presenta más fácil y rápida, aunque no suponga una indemnización para el denunciante, hacen que sea difícil encontrar sentencias sobre esta cuestión[1184].

[1182] No estoy de acuerdo con la propuesta de adopción de una postura reduccionista que sugiere algún autor, de forma que el derecho a indemnización por vulneración de la LOPD procedería sólo si se vulnerasen los derechos de la personalidad protegidos por la LO 1/1982. Esta propuesta se realiza en el marco del análisis de la responsabilidad civil por los daños causados por la inclusión indebida de datos en ficheros de morosos, que ha suscitado la aplicación del artículo 19 LOPD. Esta postura se inspira en la argumentación de GRIMALT SERVERA. Ejemplo de esta postura son: A. RUDA GONZÁLEZ, N. WILSON APONTE, "Responsabilidad civil por la inclusión de datos personales en un fichero de solvencia patrimonial", J. BALCELLS PADULLÉS, A. CERRILLO I MARTÍNEZ, M. PEGUERA POCH, I. PEÑA-LÓPEZ, M.J. PIFARRÉ DE MONER, M. VILASAU SOLANA, (Coord.). VVAA, *Internet, Derecho y Política. Una década de transformaciones. Actas del X Congreso Internacional Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona, 3-4 de julio de 2014*, Huygens Editorial, Barcelona, 2014, págs. 272 a 273.

[1183] PUYOL MONTERO considera que, aunque tiene un ámbito de aplicación distinto, la LO 1/1982 es de gran ayuda interpretativa. J. PUYOL MONTERO, "Derecho a indemnización", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, *op. cit.*, pág. 1.273. Además el TC en la diferenciación entre derecho a la intimidad y derecho a la protección de datos destacó su naturaleza de derechos afines, ya que ambos comparten el objetivo de "ofrecer una eficaz protección constitucional de la vida privada personal y familiar", STC 292/2000, de 30 de noviembre de 2000, FJ 5.

[1184] Para ilustrarlo se puede citar una sentencia del Tribunal Supremo que desestima un recurso de casación promovido por un Guardia Civil que había demandado por vulneración del derecho a la intimidad y a la propia imagen contra la Asociación Independiente de la Guardia Civil y contra el presidente de la misma por la publicación en revistas y la web de la asociación de los datos personales del funcionario demandante (currículum vitae, nombre y apellidos, domicilio, profesión, fotografía). La sentencia de primera instancia consideró acreditada la intromisión ilegítima en el derecho a la intimidad y a la propia imagen del funcionario y condenó a los demandados a abonar una indemnización. Claramente se habría podido alegar el incumplimiento de la LOPD y haber solicitado indemnización. El Guardia Civil así lo apreció pero ya en el recurso de casación, donde alegó este incumplimiento de la normativa de protección de datos. El Alto

Sin embargo, como excepción a esta aseveración, hay que mencionar el abundante número de asuntos planteados sobre ficheros de morosos en los que se solicita habitualmente indemnización. El supuesto típico es aquel en el que una entidad acreedora transmite indebidamente los datos de su presunto deudor al responsable de un fichero común.

Estos ficheros de morosos se utilizan para proporcionar información sobre la solvencia de las personas a otras entidades que pueden consultarlos antes de entablar una relación contractual con estas personas. Si los datos que figuran en estos ficheros no son veraces, puede suponer un perjuicio para las personas afectadas que pueden ver cómo se les deniegan préstamos o la posibilidad de entablar relaciones contractuales por la información contenida en los mismos. Por eso, se incluyó en la LOPD una regulación específica para este tipo de ficheros que exige ciertos requisitos para poder incluir los datos. Al acarrear perjuicios que pueden ser económicamente evaluables o que pueden traducirse en daños morales, estos asuntos son los que han originado más reclamaciones de indemnización.

El Tribunal Supremo considera que, en estos supuestos de inclusión indebida en ficheros de morosos, el derecho vulnerado es el del honor, por el desvalor social que comporta el estar incluido en estos registros como persona morosa sin serlo[1185]. Sin embargo, la vulneración de este derecho al honor se vehicula a través de la infracción de la regulación contenida en la LOPD sobre este tipo de ficheros[1186]. En consecuencia, en

Tribunal indicó que la alusión a la normativa de protección de datos no se hizo en la demanda inicial donde se accionó por vulneración de los derechos a la intimidad e imagen, siendo normas distintas las que protegen estos derechos (LO 1/1982) y la que protege el derecho a la protección de datos (LOPD), siendo pretensiones que se basan en títulos jurídicos distintos, lo que hizo que no admitiera el motivo. STS de 20 de marzo de 2013 (Sala 1ª) (ROJ: STS 2249/2013), FJ 3.

[1185] STS de 22 de enero de 2014 (Sala 1ª) (ROJ: STS 355/2014).

[1186] Entre las numerosas sentencias puede citarse como ejemplo la mencionada STS de 22 de enero de 2014 (Sala 1ª) (ROJ: STS 355/2014). En este caso, la deuda a la que se referían los datos ya se había cancelado cuando se comunicaron los datos por parte de una entidad bancaria al fichero común, por lo que el Alto tribunal considera vulnerado el principio de calidad (art. 4 LOPD). Se produce la infracción de la LOPD y se vulnera el derecho al honor. Al valorar la cuantía de la indemnización acude al artículo 9.3 LO 1/1982 (aunque también se cita el artículo 19 LOPD) que establece una presunción *iuris et de iure* de existencia de perjuicio indemnizable cuando se haya producido una intromisión ilegítima en el derecho al honor, como es el caso del tratamiento de datos personales en un registro de morosos sin cumplir las exigencias que establece la LOPD. También cabe citar la STS de 9 de abril de 2012 (Sala 1ª) (ROJ: STS 2638/2012) que versa también sobre la inclusión indebida de los datos de una persona en un fichero común de información de solvencia, el fichero de Asnef Equifax. También menciona el artículo 19 LOPD, junto al artículo 9.3 de la LO 1/1982.

estos casos de morosidad, como fundamentos jurídicos del derecho a recibir una indemnización se alegarán el artículo 9 LO 1/1982 y el artículo 19 LOPD.

Hay que recordar que el derecho a la protección de datos, además de un derecho fundamental, es un instituto de garantía de los otros derechos, en especial de los derechos a la intimidad y al honor[1187]. Es un derecho de naturaleza instrumental que permite proteger otros derechos. Como consecuencia, cuando el derecho de protección de datos actúe en virtud de esta naturaleza instrumental, podrán aplicarse las regulaciones de desarrollo de ambos derechos, el de protección de datos y el del derecho protegido.

iii. El sujeto obligado a indemnizar

El responsable y el encargado del tratamiento son los sujetos obligados a indemnizar al titular de los datos, si se cumplen los elementos que desencadenarán esta obligación. Por tanto, si el sujeto que realiza el comportamiento dañoso puede encajar en alguno de estos dos perfiles, se le considerará con legitimación pasiva ante la pretensión resarcitoria del titular de los datos. Ahora bien, hay que recordar la existencia de la dualidad en la figura de forma que tenemos dos posibles responsables: el responsable del fichero o el responsable del tratamiento. ¿Ambos pueden ser sujetos obligados a indemnizar?

Habrá que realizar una interpretación de este precepto en conexión con la definición de responsable del fichero o tratamiento (art. 3.d LOPD) y entender que ambas figuras serán sujetos obligados a indemnizar. La diferencia estará en las conductas susceptibles de generar esta obligación que dependerán de las obligaciones establecidas para estos dos sujetos[1188].

[1187] STC 292/2000, de 30 de noviembre de 2000, FJ 5.

[1188] Los supuestos que originan, como se ha comentado, más demandas civiles en las que se solicita indemnización, son los referidos a ficheros de morosos. En este contexto, la responsabilidad suele recaer en el acreedor que proporciona los datos del deudor al fichero común en virtud del incumplimiento de sus obligaciones respecto a la calidad de esos datos (art. 43 RLOPD). Hay que recordar que, como se abordó en el Capítulo III este acreedor se había considerado responsable del tratamiento (STS de 18 de julio de 2006 (Sala 3ª) (ROJ: STS 4510/2006)), en contraste con el responsable del fichero común. Pues bien, el acreedor ha sido obligado a indemnizar, entre otras en la STS de 21 de mayo de 2014 (Sala 1ª) (ROJ: STS 267/2014).

El responsable y el encargado pueden ser personas de distinta naturaleza (físicas o jurídicas de naturaleza pública o privada, órgano administrativo o entes sin personalidad jurídica). No se diferencia en la LOPD según la naturaleza del sujeto, sino que todos tienen idéntica responsabilidad. Sin embargo, se diferencia entre ficheros de titularidad pública y ficheros de titularidad privada, ya que en los primeros hay que remitirse a la legislación reguladora del régimen de responsabilidad de las Administraciones públicas y, por tanto, regirá lo dispuesto en esta regulación[1189].

En lo referente a los ficheros de titularidad pública la Constitución española establece un principio de responsabilidad de las Administraciones públicas, de forma que "los particulares, en los términos establecidos por la ley, tendrán derecho a ser indemnizados por toda lesión que sufran en cualquiera de sus bienes y derechos, salvo en los casos de fuerza mayor, siempre que la lesión sea consecuencia del funcionamiento de los servicios públicos" (art. 106.2 CE). La ley que desarrolló este precepto constitucional fue la Ley 30/1992 de régimen jurídico de las administraciones públicas y del procedimiento administrativo común.

En cuanto a ficheros de titularidad privada, en el régimen del Código civil, las personas jurídicas se han considerado responsables, no sólo en virtud de la asunción de obligaciones contractuales sino también como sujetos susceptibles de indemnizar daños extracontractuales[1190]. En este último ámbito, la responsabilidad extracontractual de la persona jurídica no sólo se ha considerado derivada de los daños que pudieran ocasionar sus dependientes (ex art. 1903 Cc) sino también por los que pudieran ocasionar sus representantes, que se reputan como propios.

[1189] Como señala FERNÁNDEZ SALMERÓN aparentemente hay una contradicción entre los apartados primero y segundo del artículo 19 LOPD, ya que en el primero condiciona de forma general el nacimiento de la obligación resarcitoria a que se haya producido un incumplimiento de la LOPD y en el segundo se indica que cuando los daños se produzcan respecto a ficheros de titularidad pública, el régimen jurídico aplicable será el de la responsabilidad patrimonial de las administraciones públicas. En este último caso, la responsabilidad no nace por la ilegalidad de una actuación, sino por el mero funcionamiento de los servicios públicos. Por eso hay que solventar esta aparente contradicción al entender que la regulación del primer apartado del artículo 19 se refiere a los daños ocasionados por particulares y no a los originados por las administraciones públicas que se regirán por su normativa específica. M. FERNÁNDEZ SALMERÓN, *La protección de los datos personales en las Administraciones Públicas*, *op. cit.*, págs. 446 a 447.

[1190] E. GÓMEZ CALLE, "Capítulo VI. Los sujetos de la responsabilidad civil. La responsabilidad por hecho ajeno", L.F. REGLERO CAMPOS (Coord.), VVAA, *Tratado de responsabilidad civil, Tomo I Parte General*, *op. cit.*, págs. 1.008 a 1.014.

Pero además incluso se ha atribuido responsabilidad a la persona jurídica respecto a aquellos daños que no se pudieran imputar a nadie derivados del mal funcionamiento en la organización de la actividad (ambos supuestos ex art. 1902 Cc)[1191]. Así, en este último caso, cuando la persona jurídica presta servicios mediante una organización de medios materiales y personales de gran complejidad, como un hospital, se pueden producir daños derivados del mal funcionamiento o de la organización de la actividad que también se atribuyen a la persona jurídica, incluso aunque no se pueda individualizar al causante de los daños[1192].

Entiendo que, en el régimen de la LOPD, claramente se ha optado por considerar a cualquier sujeto colectivo, incluso el que no tenga personalidad jurídica, obligado a indemnizar con las únicas limitaciones que suponen: el encaje en la definición de responsable o de encargado y la conexión de la conducta que supone el incumplimiento a este sujeto.

La definición de responsable del fichero o del tratamiento se rectificó en el RLOPD para contemplar la posibilidad de que actuara "sólo o conjuntamente con otros" (art. 5.1.q RLOPD). Sin embargo, pese a existir este componente de corresponsabilidad no se han establecido reglas sobre la forma en que se responderá en estos casos. No obstante, la jurisprudencia estima que, al igual que sucede en el régimen general de la responsabilidad extracontractual contemplado en el Código civil[1193], prevalece el criterio de responsabilidad solidaria.

Como ejemplo de este criterio, hay que citar una sentencia del Tribunal Supremo ya mencionada[1194]. El asunto se refería a la inclusión de los datos de un ciudadano en un fichero de información sobre solvencia. El Tribunal Supremo estimó que, tanto la entidad que había facilitado los datos inexactos al titular del fichero, como éste mismo, que había denegado el derecho de cancelación, debían responder civilmente de forma solidaria[1195].

[1191] *Ibídem.*
[1192] *Ibídem.*
[1193] C.I. ASÚA GONZÁLEZ, "La responsabilidad(I)", L. PUIG I FERRIOL, M.C. GETE-ALONSO Y CALERA, J. GIL RODRÍGUEZ, J.J. HUALDE SÁNCHEZ, *Manual de derecho civil II, derecho de obligaciones, responsabilidad civil, teoría general del contrato, op. cit.*, pág. 464.
[1194] STS de 21 de mayo de 2014 (Sala 1ª) (ROJ: STS 267/2014).
[1195] BUSTO LAGO considera, sin embargo, que deben diferenciarse dos supuestos. El primero sería el que implica que el poder de decisión sobre el tratamiento de datos corresponde a cada uno de los responsables en su totalidad, por lo que la responsabilidad se atribuiría a todos ellos de forma indistinta y solidaria. El

El Alto Tribunal argumentó que ambos eran responsables, contrariamente a lo que había resuelto el juzgado de primera instancia que había estimado que la empresa titular del fichero común había cumplido con lo previsto en la legislación y no debía responder.

iv. Los daños

El daño debe ser injusto, ya que pueden ocasionarse daños que la víctima deba soportar[1196]. En este sentido, si la LOPD establece un deber para el responsable cuyo cumplimiento pueda conllevar la producción de un daño para el titular, éste deberá soportarlo y no se considerará indemnizable.

Respecto al daño también hay que tener en cuenta que no cabrá considerar que hay responsabilidad si quien causa el daño lo hace amparado por una causa de justificación, lo que excluiría la antijuricidad del daño, como puede ser: el estado de necesidad, la legítima defensa, el consentimiento del ofendido y el ejercicio legítimo de un derecho (tanto si se trata de confrontar derechos como de límites del ejercicio legítimo del derecho)[1197].

Para valorar los daños, como ya se ha mencionado anteriormente, algunos autores consideran aplicable lo establecido por la LO 1/1982. Cuando el derecho a la protección de datos funciona como garantía de otros derechos, como los de honor o intimidad, al existir una doble vulneración, es razonable que se utilicen los criterios que establece la LO 1/1982 para hacer la valoración de los daños, máxime cuando la LOPD no introduce ningún criterio. Ahora bien, el hecho de utilizar los criterios de la LO 1/1982 cuando el único derecho vulnerado sea el de protección de datos, es una cuestión pragmática que

segundo implicaría que los diferentes responsables deciden sobre diferentes aspectos del tratamiento de datos. En este segundo caso, el autor entiende que no cabría la exoneración de responsabilidad ya que se trataría de un pacto no oponible a terceros ex artículo 1257 Cc y contrario al orden público, límite a la autonomía privada ex artículo 1255 Cc. Cita para apoyar su tesis a P. GRIMALT SERVERA, *La responsabilidad civil en el tratamiento automatizado de datos personales, op. cit.*, pág. 121. J.M. BUSTO LAGO, "La responsabilidad de los responsables de ficheros de datos personales y de los encargados de su tratamiento", *Revista Aranzadi Civil-Mercantil, op. cit.* págs. 7 a 8.

[1196] R. DE ÁNGEL YAGÜEZ, "La responsabilidad civil. Cuestiones previas de delimitación", I. SIERRA GIL DE LA CUESTA, R. DE ÁNGEL YAGÜEZ [et al.] (Coord.), VVAA, *Tratado de responsabilidad civil, op. cit.*, pág. 12.

[1197] F. PEÑA LÓPEZ, "Capítulo II. De las obligaciones que nacen de culpa o negligencia", R. BERCOVITZ RODRÍGUEZ-CANO, VVAA, *Comentarios al Código Civil, Tomo IX*, Tirant lo Blanch, Valencia 2013, pág. 12.968 a 12.970.

decide el juzgador, pero ya no puede fundamentarse en que estamos ante el derecho a la intimidad, consideración superada ya[1198].

Ante la ausencia de mención expresa en el artículo 19 LOPD se ha suscitado si el daño susceptible de indemnización incluiría el daño moral. La doctrina y la jurisprudencia han entendido que también deben cubrirse los posibles daños morales, ya que, en caso contrario, estaría muy limitado el derecho a indemnización del artículo 19 LOPD[1199]. No obstante, debería tenerse en cuenta que, pese a no contar con criterios para determinar este daño en el precepto, ello tampoco debería llevar al extremo contrario de considerar automáticamente que existe daño moral lo que llevaría a una patrimonialización del derecho, al igual que sucede con los derechos protegidos por la LO 1/1982[1200].

[1198] J. PUYOL MONTERO, "Derecho a indemnización", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, *op. cit.*, pág. 1.273. A. ORTÍ VALLEJO, *Derecho a la intimidad e informática (Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada)*, *op. cit.*, págs. 166 a 171. Este autor además apunta a que, si bien, la determinación del daño moral es discrecional del juzgador, se podrían utilizar los criterios de valoración del daño moral de la LO 1/1982 con relación al supuesto del artículo 17.3 LORTAD (antecedente del art. 19 LOPD). También considera que se podrían aplicar los criterios de valoración de la LO 1/1982 a la indemnización de la LOPD: M.R. LLÁCER MATACÁS, *La autorización al tratamiento de información personal en la contratación de bienes y servicios. La privacidad, entre el estatuto del responsable y la fragilidad del consentimiento*, *op. cit.*, pág. 124. La SAP Barcelona de 17 de julio de 2014 (Sección 16) (ROJ: SAP B 8246/2014) que entiende afectados también los derechos al honor y a la intimidad, considera que el núcleo de la controversia suscitada se refiere al derecho a la protección de datos. Por ello, entra a valorar los daños ocasionados por el incumplimiento de la LOPD. La Audiencia, ante la dificultad "patente" de cuantificar el daño moral, opta por utilizar los criterios del artículo 9.3 LO 1/1982 a efectos orientativos (y se remite a la STS de 21 de mayo de 2014 (Sala 1ª) (ROJ: STS 267/2014)) que también los había utilizado aunque en un asunto relativo a ficheros de morosos). Finalmente la Audiencia, tras valorar los daños morales generados por el incumplimiento de la LOPD, alude a los daños generados por la intromisión ilegítima en los derechos al honor y a la intimidad. Como en la demanda no se diferenció entre estos derechos al pedir la indemnización, la Audiencia decide no diferenciar en sentencia y estima que el importe valorado cubre las vulneraciones de todos los derechos (FFJJ 27 a 29).

[1199] Así, por ejemplo la SAP Barcelona de 17 de julio de 2014 (Sección 16) (ROJ: SAP B 8246/2014) estima que no pueden constatarse daños patrimoniales pero sí daños morales.

[1200] A. ORTÍ VALLEJO, *Derecho a la intimidad e informática (Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada)*, *op. cit.*, págs. 166 a 171. Como indicaba ORTÍ VALLEJO se correría el riesgo de que se concedan indemnizaciones ante cualquier irregularidad en la utilización de los datos sin analizar si cabe o no que exista daño moral. Considera HERRÁN ORTIZ que ello no debe obstar al reconocimiento de este derecho a la indemnización, lo que apoya M.C. GUERRERO PICÓ, *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, *op. cit.*, pág. 309. A.I. HERRÁN ORTIZ, *El Derecho a la intimidad en la nueva ley orgánica de protección de datos personales*, Dykinson, Madrid, 2002, pág. 260. Curiosamente este vaticinio que realizaba ORTÍ VALLEJO hace 20 años no se ha cumplido respecto al derecho de indemnización, poco utilizado en el ámbito del derecho a la protección de datos pero sí se utiliza la vía administrativa como instrumento muchas veces de presión contra el responsable del tratamiento para resolver cuestiones que nada tienen que ver con la defensa de este derecho.

En la jurisprudencia hallamos ejemplos de aplicación de los criterios contenidos en el artículo 9.3 LO 1/1982 que extiende claramente la indemnización al daño moral[1201]. Así, se puede citar un asunto sobre el llamado "derecho al olvido", en el que la Audiencia Provincial de Barcelona valoraba los daños morales producidos por la publicación en el servicio de búsquedas de *Google* de un enlace al BOE, donde aparecía el indulto otorgado al recurrente por un delito contra la salud pública[1202].

La Audiencia en función de los criterios de la LO 1/1982 y lo indicado por el Tribunal Supremo en un asunto sobre ficheros de morosos[1203], estimó como criterios aplicables a este caso: la afectación de la dignidad del demandante por la naturaleza de la información divulgada, la publicación como resultado del poderoso buscador *Google*, el quebranto derivado de las dificultades para conseguir la supresión y la duración del daño atribuible a la demandada[1204].

v. Títulos de imputación

Los títulos de imputación responderían a la pregunta: ¿por qué se responde? La doctrina civil proporciona dos posibles respuestas. Puede considerarse que el autor del daño responde porque se ha producido por su culpa. La actuación de este sujeto que ha producido el daño ha sido decidida por él consciente de que podía o iba a producir ese daño. Otra opción es entender que responde el autor del daño porque es quien lo causa, con independencia de que haya tenido o no culpa de que se produzca. En esta segunda posibilidad, el autor debe indemnizar el daño sólo por haberlo ocasionado o por haber realizado una actividad apta para producir un riesgo que se ha materializado finalmente en la producción de un daño[1205].

[1201] Los criterios que establece el artículo 9.3 LO 1/1982 para valorar este daño moral son: las circunstancias del caso y la gravedad de la lesión efectivamente producida, para lo que se tendrá en cuenta, en su caso, la difusión o audiencia del medio a través del que se haya producido.
[1202] SAP Barcelona de 17 de julio de 2014 (Sección 16) (ROJ: SAP B 8246/2014).
[1203] El Tribunal Supremo consideró indemnizable, como daño moral "en primer lugar la afectación a la dignidad en su aspecto interno o subjetivo, y en el externo u objetivo relativo a la consideración de las demás personas. Para calibrar este segundo aspecto ha de verse la divulgación que ha tenido tal dato". También considera indemnizable el "quebranto y la angustia producida por el proceso más o menos complicado que haya tenido que seguir el afectado para la rectificación o cancelación de los datos incorrectamente tratados", STS de 22 de enero de 2014 (Sala 1ª) (ROJ: STS 355/2014).
[1204] SAP Barcelona de 17 de julio de 2014 (Sección 16) (ROJ: SAP B 8246/2014), FJ 28.
[1205] R. DE ÁNGEL YAGÜEZ, "Fundamento de la responsabilidad civil. Culpa y riesgo. Responsabilidad objetiva. Regímenes especiales de responsabilidad", I. SIERRA GIL DE LA CUESTA, R. DE ÁNGEL YAGÜEZ [et al.] (Coord.), VVAA, *Tratado de responsabilidad civil*, *Tomo I*, *op. cit.*, pág. 126. Ilustra este

La primera opción representaría la responsabilidad subjetiva fundada en la idea de culpa y que ha sido la adoptada por nuestro Código civil (art. 1902 Cc). La segunda opción es la correspondiente a la responsabilidad objetiva o sin culpa.

Si bien tradicionalmente la responsabilidad se ha fundamentado en la culpa, el desarrollo industrial del siglo XIX y el aumento de actividades peligrosas que provocaron un aumento de las víctimas de daños, originó una transformación en la aplicación e interpretación del principio de culpa hacia lo que se conoce como cuasi-objetivación de la responsabilidad[1206].

Esta cuasi-objetivación de la responsabilidad subjetiva consta de los siguientes presupuestos establecidos por la jurisprudencia: a) el incremento de los niveles de diligencia exigidos; b) la inversión de la carga de la prueba, de forma que una vez acreditado el hecho dañoso y sus consecuencias le incumbe al autor probar que obró con diligencia debida; c) la invocación de la idea del riesgo creado como argumento de cara a la atribución de responsabilidad[1207].

Paralelamente han aparecido leyes específicas que incluyen disposiciones orientadas a resarcir a quienes sufran un daño sin importar si ha habido culpa o no por

---

autor las dos opciones con un ejemplo muy claro. En la primera opción de responsabilidad fundada en la culpa, el conductor que arrolla a un peatón porque le fallan los frenos no respondería pero sí lo haría en la segunda opción de responsabilidad sin culpa, por el sólo hecho de haber causado el daño o, si se quiere, de haber decidido poner en funcionamiento el vehículo generador de un riesgo.

[1206] C.I. ASÚA GONZÁLEZ, "La responsabilidad(I)", L. PUIG I FERRIOL, M.C. GETE-ALONSO Y CALERA, J. GIL RODRÍGUEZ, J.J. HUALDE SÁNCHEZ, *Manual de derecho civil II, derecho de obligaciones, responsabilidad civil, teoría general del contrato, op. cit.*, pág. 466. Sin embargo, hay que matizar que la doctrina es algo confusa en lo que se refiere a la responsabilidad objetiva y la cuasi-objetivación. Así, PEÑA LÓPEZ señala que actualmente la aplicación de la responsabilidad objetiva está en retroceso. De esta forma, indica que el Tribunal Supremo ante una actividad generadora de riesgos considerablemente superiores a los estándares normales aplica la "doctrina del riesgo" y cuando la actividad no genera riesgos especiales aplica la responsabilidad por culpa. F. PEÑA LÓPEZ, "Capítulo II. De las obligaciones que nacen de culpa o negligencia", R. BERCOVITZ RODRÍGUEZ-CANO, *Comentarios al Código Civil, Tomo IX, op.cit.*, págs. 12.978 a 12.979. Sin embargo, O'CALLAGHAN, de forma radicalmente opuesta, deja claro que la tendencia a la objetivación es imparable, de forma que "se desplaza la culpabilidad al nexo causal; la acción se califica por la culpa y ésta se sustituye por el riesgo". Destaca gráficamente este autor que la doctrina acerca de la responsabilidad extracontractual no es que esté en desacuerdo en algunos puntos sino que no está de acuerdo en nada, por lo que estima más adecuado fijarse en la jurisprudencia que claramente tiende a la responsabilidad objetiva según el autor. X. O'CALLAGHAN MUÑOZ, "La responsabilidad objetiva", J.A. MORENO MARTÍNEZ (Coord.), VVAA, *La responsabilidad civil y su problemática actual*, Dykinson, Madrid, 2007, págs. 800 a 820.

[1207] C.I. ASÚA GONZÁLEZ, "La responsabilidad(I)", L. PUIG I FERRIOL, M.C. GETE-ALONSO Y CALERA, J. GIL RODRÍGUEZ, J.J. HUALDE SÁNCHEZ, *Manual de derecho civil II, derecho de obligaciones, responsabilidad civil, teoría general del contrato, op. cit.*, págs. 466 a 467.

parte del autor del mismo, como la legislación de prevención de riesgos laborales o la Ley de sobre responsabilidad civil y seguro en la circulación de vehículos a motor[1208]. De esta forma, estas leyes han recogido fórmulas de responsabilidad objetiva[1209]. En estas fórmulas lo que se examinará básicamente es si existe un nexo causal entre la conducta del sujeto y el daño ocasionado a la víctima.

¿Cuál es el tipo de responsabilidad que contempla la LOPD? ¿Se trata de una responsabilidad objetiva o subjetiva, o hay que entender que es subjetiva pero sujeta a la cuasi-objetivación comentada?

La respuesta no es fácil, ya que ni la doctrina ni la jurisprudencia son suficientemente claras[1210]. Sin embargo, es importante analizarlo, ya que depende del enfoque que se adopte tendrá repercusiones en la forma en la que el responsable podrá o no defenderse de la demanda de responsabilidad. Asimismo puede repercutir en la preparación de la estrategia procesal del responsable.

En principio, la idea de riesgo parece enteramente aplicable al contexto del derecho a la protección de datos, ya que la utilización por parte de los responsables de los avances de la tecnología para obtener un beneficio acarrearía un riesgo para los titulares de los datos. Sin embargo ¿qué organización no utiliza las tecnologías hoy en día? ¿Todas las actividades deben incorporarse a esta idea de riesgo?[1211]

Se podría establecer una graduación en el riesgo que dependiera de la intensidad del uso de la tecnología o de los datos afectados. Así, por ejemplo, los avances recientes

[1208] Real Decreto Legislativo 8/2004, de 29 de octubre, por el que se aprueba el texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor (BOE núm. 267 de 5.11.2004).
[1209] R. DE ÁNGEL YAGÜEZ, "Fundamento de la responsabilidad civil. Culpa y riesgo. Responsabilidad objetiva. Regímenes especiales de responsabilidad", I. SIERRA GIL DE LA CUESTA, R. DE ÁNGEL YAGÜEZ [et al.] (Coord.), VVAA, *Tratado de responsabilidad civil, Tomo I, op. cit.*, pág. 128.
[1210] Como indica PUYOL MONTERO se echa de menos una mayor concreción en el alcance de la responsabilidad de la LOPD. J. PUYOL MONTERO, "Derecho a indemnización", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, pág. 1.282.
[1211] Para DÍEZ-PICAZO la responsabilidad por riesgo debería atañer a los empresarios en el círculo de su actividad empresarial, de forma que comprendieran los riesgos típicos de la empresa, los que su actividad lleve consigo. Habría, dentro de esta línea dos posibilidades: una sería atribuir la responsabilidad por riesgo al uso de las nuevas tecnologías o a las consecuencias de la multiplicación del maquinismo y otra sería atribuirla a aquellos supuestos en lso que la actividad resulte peligrosa por sí misma, de acuerdo con las pautas de la experiencia. L. DÍEZ-PICAZO, *Fundamentos del derecho civil patrimonial. V La responsabilidad civil extracontractual*, *op.cit.*, pág. 283.

en análisis de grandes volúmenes de datos (lo que se conoce como *Big data*) podrían suponer este riesgo acrecentado para los titulares de los datos, al lado del beneficio de quienes utilizan los resultados de estos análisis. En otro nivel situaríamos a aquellas organizaciones que utilizarían los datos personales para actividades habituales que, por tanto, no generarían especiales riesgos.

No obstante, sin ahondar en estas reflexiones, lo que parece razonable es que se opte por entender que la responsabilidad *a priori* en esta materia pueda ser calificada de objetiva o a lo sumo de subjetiva cuasi-objetivada.

Entiendo que si la LOPD hubiera establecido que cualquier tratamiento de datos que produzca un daño originara la obligación de indemnizar del responsable o del encargado del tratamiento, sería claramente un caso de responsabilidad objetiva[1212]. Por otro lado, tampoco se contienen títulos de imputación en el artículo 19 LOPD, sino que el desencadenante de la obligación de indemnizar es el incumplimiento legal.

Si acudimos al principal referente de la defensa de la responsabilidad objetiva, GRIMALT SERVERA[1213], se centra precisamente en este incumplimiento legal que

[1212] Este era el supuesto que se contemplaba en el inicio del trámite de elaboración de la Directiva 95/46/CE cuando la responsabilidad se originaba por un daño ocasionado por el tratamiento de datos (art. 21 Propuesta de Directiva de 1990). GRIMALT SERVERA también señala que si se hubiera contemplado en la LORTAD que el mero hecho de realizar un tratamiento de datos originara la obligación de indemnización si se produjera un daño, sería claramente una responsabilidad objetiva plena. P. GRIMALT SERVERA, *La responsabilidad civil en el tratamiento automatizado de datos personales*, *op.cit.*, pág. 147.

[1213] Siguen los postulados de GRIMALT SERVERA: BUSTO LAGO, que tras exponer las diversas posturas doctrinales acoge la de GRIMALT SERVERA con apoyo en la interpretación de la Directiva 95/46/CE; LAGUNA REYES, que se refiere al trabajo de BUSTO LAGO; EGUSQUIZA BALMASEDA y HERRÁN ORTIZ. HEREDERO HIGUERAS entiende que lo que quiso recoger el legislador en el artículo 19 LOPD, aún sin saberlo, es la responsabilidad objetiva y para ello se remite al antecedente del precepto que lo sitúa en la Ley federal alemana de 1990, según se ha comentado antes al abordar la elaboración de la Directiva 95/46/CE. ORTEGA GIMÉNEZ simplemente califica la responsabilidad de objetiva, sin remisión a ningún autor ni más argumentación. J.M. BUSTO LAGO, "La responsabilidad de los responsables de ficheros de datos personales y de los encargados de su tratamiento", *Revista Aranzadi Civil-Mercantil* núm. 5, 2006, págs. 1 a 40; L. LAGUNA REYES, *Responsabilidad civil derivada de la inclusión indebida en un registro de morosos*, Trabajo fin de Máster Universitario Acceso a la Abogacía, M.L., ARCOS VIEIRA (Directora), Universidad Pública de Navarra, 2014, http://hdl.handle.net/2454/9628, (fecha consulta: 10.7.2014), págs. 42 a 45; M.A. EGUSQUIZA BALMASEDA, "Aspectos civiles de la protección de datos", *Publicaciones del Consejo General del Poder Judicial: Monografías. Cuadernos digitales de Formación. Recursos electrónicos*, CGPJ nº29, Madrid, 2012, pág. 33; A.I. HERRÁN ORTIZ, *El Derecho a la intimidad en la nueva ley orgánica de protección de datos personales*, *op. cit.*, págs. 258 a 261; M. HEREDERO HIGUERAS "Ensayo sobre la regulación de la responsabilidad y administrativa en la LO 15/1999 de protección de datos de carácter personal", TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, *op. cit.*, pág. 2.179; A. ORTEGA GIMÉNEZ, "Cloud computing, protección de datos y derecho internacional privado (resolución de

considera que es el criterio de imputación[1214]. Es decir, a la pregunta ¿por qué debe responder el responsable? Contesta el autor: porque se ha incumplido la LOPD. Sea quien sea el que ha incumplido, si ha habido incumplimiento y, de éste ha derivado un daño a los bienes o derechos del afectado, el responsable deberá indemnizar los perjuicios con independencia de la concurrencia de la culpa. Así, GRIMALT SERVERA califica esta responsabilidad como objetiva pero limitada por el hecho del incumplimiento objetivo de las disposiciones de la LORTAD, actualmente LOPD[1215].

En vez de ligar la obligación de indemnizar a la conducta del responsable que origina el incumplimiento, lo que hace este autor es conectarla al incumplimiento directamente. GRIMALT SERVERA defiende la utilidad de su interpretación porque así pretende esquivar la posibilidad de que se apliquen otras reglas externas a la LOPD y además asegura que el responsable responda aún en casos de responsabilidad por hecho ajeno, de los que podría evitar responder si se aplicara el régimen del Cc.

Como argumentos a favor de esta postura esgrime los debates parlamentarios sobre esta cuestión durante la preparación de la LORTAD y la configuración de la responsabilidad en la Propuesta de Directiva de 1990.

En los debates parlamentarios se introduce, como ejemplo de lo que se persigue con el texto del precepto dedicado al derecho de indemnización, un supuesto claro de responsabilidad objetiva: el del dueño de la casa que responde de los daños causados por las cosas que se arrojaren o cayeren de la misma (art. 1.910 Cc) [1216]. Sin embargo, en ese

---

controversias y determinación de la ley aplicable)", R. MARTÍNEZ MARTÍNEZ (Ed.), *Derecho y cloud computing*, Aranzadi, Cizur Menor (Navarra), 2012, págs. 261 a 262.

[1214] P. GRIMALT SERVERA, *La responsabilidad civil en el tratamiento automatizado de datos personales*, *op.cit.*, pág. 147.

[1215] En el momento en que GRIMALT SERVERA realiza su monografía estaba vigente la LORTAD, aunque el artículo 17.3 LORTAD era prácticamente idéntico al artículo 19 LOPD excepto porque n incluía a los encargados del tratamiento, por no existir esa figura en la LORTAD.

[1216] Así, respecto al artículo 17.3 LORTAD (como el precepto se ha mantenido inalterado prácticamente en la LOPD, hay que acudir al proceso de elaboración de la LORTAD para entender las razones de su incorporación), menciona GRIMALT SERVERA que se acogió lo indicado por el Sr. Merino Navarrete: "[…] en el interior del fichero habrá ocurrido lo que sea, el causante del atropello del ordenamiento jurídico, de los bienes o derechos protegidos, será quien sea, pero aquí hay una persona que responde y, para que no haya ninguna duda, es el que las leyes denominan responsable. Evidentemente, en ciertos casos el responsable va a cargar con una especie de responsabilidad como la del dueño de la casa de la que se cae una maceta, a pesar de que su falta de voluntad que ocurra porque la ha tirado un niño o quien sea, pero paga el dueño de la casa; bueno pues aquí igual, aunque luego, se podrá repercutir contra el dependiente. No quiero llegar al análisis jurídico para determinar si es posible que el afectado pueda dirigirse al mismo tiempo contra el dependiente; digo que la ley quiere fijar desde el principio cuál es la legitimación pasiva en

debate también se mencionaba la posibilidad de ir contra el dependiente (es decir *ex* art. 1903 Cc), lo que sería argumento para apoyar la tesis contraria.

Respecto a la propuesta inicial de la Directiva 95/46/CE ya se comentó que la responsabilidad objetiva se fue diluyendo durante el proceso de tramitación hasta llegar a la versión final en la que se pueden defender diversas posturas.

Estoy de acuerdo con GRIMALT SERVERA en que es necesario limitar la obligación de indemnizar a los supuestos derivados de la LOPD, ya que hay que entender que nos hallamos ante un sistema típico de responsabilidad. Está claro que las conductas que deben originar este deber son aquellas que ocasionen el incumplimiento legal y su valoración debe realizarse en el contexto de la LOPD[1217]. Cuestión diferente es que esta valoración deben realizarla los tribunales civiles de acuerdo con sus propios criterios, que, como ya se ha comentado, podrán no ser los mismos que se tienen en cuenta en el ámbito sancionador administrativo[1218].

También queda claro que el sujeto obligado a indemnizar se ha delimitado, de forma que será el responsable o el encargado del tratamiento. Entiendo que lo que los debates parlamentarios durante la tramitación de la LORTAD reflejaban y la finalidad misma de la creación de estas figuras es precisamente conseguir "un chivo expiatorio" que indemnice en caso de producirse un daño derivado del incumplimiento ocasionado en el marco de sus organizaciones[1219].

En definitiva, lo que en ningún caso debe establecerse ni tiene ningún apoyo es que debamos optar por una responsabilidad claramente subjetiva. El titular de los datos, víctima del daño, no debe acreditar la concurrencia en el responsable de dolo o culpa,

---

un proceso indemnizatorio y lo dice con toda claridad […]. Dictamen de la Comisión Constitucional a la vista del informe elaborado por la Ponencia, sobre el Proyecto de Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal (BOCG, Serie A, nº 59-1, de 24-7-91)(número de expediente 121/000059) (continuación). Cortes Generales, Diario de sesiones del Congreso de los Diputados, Comisiones, Constitucional, IV Legislatura, nº 425, sesión de 8 de abril de 1992, págs. 12536-12537, citado en P. GRIMALT SERVERA, *La responsabilidad civil en el tratamiento automatizado de datos personales*, *op.cit.* págs. 150 a 154.

[1217] STS de 30 de marzo de 2011 (Sala 1ª) (ROJ: STS 2227/2011), FJ 3.

[1218] STS de 21 de mayo de 2014 (Sala 1ª) (ROJ: STS 267/2014), FJ 8.

[1219] E. DEL PESO NAVARRO, M.A. RAMOS GONZÁLEZ, *Confidencialidad y seguridad de la información: la LORTAD y sus significaciones socioeconómicas*, Díaz de Santos, Madrid, 1994, págs. 103 a 104.

sino que bastaría que probara el daño y el nexo causal entre la conducta incumplidora del responsable y el daño[1220]. De esta forma, en la práctica, lo que sucede es que los tribunales, una vez han establecido que ha existido un incumplimiento y que existen unos daños, analizan si existe el nexo causal[1221].

Lo que quedaría por resolver es si el responsable puede acreditar que ha actuado con la diligencia debida y, por tanto, estamos en una responsabilidad subjetiva a la que aplicaríamos los requisitos de la cuasi-objetivación. O si, por el contrario, una vez se acredite que se ha incumplido la LOPD, el responsable debe indemnizar, sin que se admita la posibilidad de que pruebe que ha actuado con la diligencia debida[1222]. En este último caso, sólo podrá alegar para excluir su responsabilidad que no existe nexo causal. Para ello, creo que hay que estar a la configuración de la obligación legal. Es importante que se motive al responsable a cumplir con sus obligaciones y se premie a quien procure actuar diligentemente. En este sentido, la tendencia a la autorregulación mediante la elaboración de códigos tipo puede incentivarse si realmente ayuda al responsable cumplidor de estas buenas prácticas a reducir o evitar que deba indemnizar.

[1220] GRIMALT SERVERA mantiene que el afectado debe probar el incumplimiento, al tratarse de un hecho constitutivo (art. 1.214 Cc) aunque advierte que podría aplicarse la inversión de la carga de la prueba, uno los expedientes utilizados por el Tribunal Supremo para objetivar la culpa. Sorprende esta mención efectuada en nota al pie de página, ya que probar el incumplimiento será ir más allá de probar el daño y el nexo causal. Este autor no deja claras las consecuencias de su tesis en la práctica. P. GRIMALT SERVERA, *La responsabilidad civil en el tratamiento automatizado de datos personales, op.cit.,* pág. 153. LLÁCER que entiende que se debe partir de una responsabilidad subjetiva, entiende que la culpa va implícita en el incumplimiento y que respecto a la prueba, sobre el afectado recae la carga de probar el daño y la relación de causalidad y al responsable probar que ha observado la diligencia perita para evitar el daño. M.R. LLÁCER MATACÁS, *La autorización al tratamiento de información personal en la contratación de bienes y servicios. La privacidad, entre el estatuto del responsable y la fragilidad del consentimiento, op. cit.*, pág. 121.

[1221] La Audiencia Provincial de Barcelona consideró que "El incumplimiento de la normativa de protección de datos no implica automáticamente un daño o lesión indemnizable". Así, la Audiencia analizaba si existía el nexo causal entre el daño alegado por el recurrente y la conducta del responsable que había supuesto el incumplimiento legal. Por ejemplo, la Audiencia considera que el fracaso de un negocio no puede conectarse con la publicación por *Google* de un indulto relacionado con un delito contra la salud pública durante diez meses en el año 2010. SAP Barcelona de 17 de julio de 2014 (Sección 16) (ROJ: SAP B 8246/2014).

[1222] PUYOL MONTERO, respecto a la tesis de naturaleza objetiva, plantea la interpretación de los niveles de exigencia en el cumplimiento de las obligaciones legales, ya que considera que puede llegar a convertir en un hecho tan injusto para el responsable, como el que pueda sufrir el afectado ante una vulneración de sus derechos. Por lo que hace un llamamiento a la mesura a la hora de ponderar el régimen de imputación y de responsabilidad. Coincido con PUYOL MONTERO pero creo que esta situación se corrige mediante la valoración que los tribunales hacen del incumplimiento, de forma que pueden tener en cuenta la naturaleza de la obligación legal. J. PUYOL MONTERO, "Derecho a indemnización", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.,* pág. 1283.

Si la obligación se configura como una obligación de medios (como la de cumplir con las debidas medidas de seguridad), tiene que permitirse al responsable poder probar que ha observado la diligencia debida y debe entenderse que se trata de una responsabilidad subjetiva[1223]. No obstante, resulta coherente con el contexto descrito en el que se desenvuelve el tratamiento de datos que se apliquen los presupuestos comentados de la cuasi-objetivación de la responsabilidad.

En este sentido se puede mencionar una sentencia en la que la Audiencia Provincial de Cádiz estimó que el responsable de un fichero de morosos (Asnef) había acreditado que actuó conforme a lo establecido en la LOPD[1224]. En cambio la Audiencia considera que la entidad bancaria que proporcionó los datos a Asnef actuó negligentemente lo que ocasionó el daño consistente en que los datos pudieron ser consultados por otras entidades. Asimismo, la Audiencia afirmó que incumbía la carga de la prueba a las víctimas[1225].

[1223] En esta línea iba la tesis sostenida por ORTÍ VALLEJO en referencia al artículo 17.3 LORTAD que consideraba que la responsabilidad era objetiva, excepto para los supuestos de incumplimiento de la obligación de seguridad, en los que entendía que la responsabilidad era subjetiva ya que admitía que el responsable probara su diligencia. Esta postura entiendo que la adoptó a raíz de los primeros textos de la Directiva 95/46/CE (Propuesta de Directiva de 1990 y Propuesta de Directiva de 1992) en los que se contemplaba la posibilidad de probar de exoneración de responsabilidad si se probaba la diligencia en materia de medidas de seguridad. A. ORTÍ VALLEJO, *Derecho a la intimidad e informática (Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada)*, *op. cit.*, págs. 166 a 171.

[1224] SAP Cádiz de 27 de octubre de 2006 (Sección 8) (ROJ: SAP CA 2463/2006), FJ 6, 8.

[1225] Como ejemplo también se puede mencionar otro asunto en el que la víctima había demandado a AUNA, operadora de telefonía, que comunicó sus datos a un fichero de morosos. En el juicio se consideró acreditado que se había suplantado la personalidad de esta víctima, lo que había ocasionado una deuda. Tras establecer que hubo incumplimiento de la LOPD, la Audiencia estimó que "La responsabilidad de la demandada se deriva de su falta de diligencia" "de haber obrado diligentemente la hoy demandada, debió haber interrumpido la preasignación, pues no contaba, ni con una relación contractual, ni con el consentimiento de la titular de los datos" "ni antes ni después de la irregularidad obviada por la demandada, obró con la prudencia y diligencia adecuadas y exigibles a una entidad profesional del sector, especialmente en lo que respecta al manejo de datos personales en los que un eventual error, cual sería el caso derivado de una suplantación de personalidad, podía dar lugar a infracciones del derecho al honor". Sin embargo la Audiencia rebaja la indemnización por daño moral, entre otras cuestiones, porque la víctima no llegó a acreditar que el daño tuviera la relevancia que pretendía ni que provocara ninguna denegación de financiación, SAP Islas Baleares de 30 de junio de 2006 (Sección 4) (ROJ: SAP IB 1569/2006), FJ 4, 5. Asimismo, también en otro asunto sobre una indebida inclusión de datos en un fichero de morosos, pese a que la Audiencia manifiesta que la responsabilidad es objetiva, luego indica "Debiendo recordar que la entidad demandada no ha aportado documento alguno, pese a que a ella le incumbía, sobre el cumplimiento del requisito que acredite la verificación del requerimiento previo de pago; de la totalidad de la documentación aportada por la demandada no se puede ni siquiera inferir indiciariamente que se hubiese cumplido dicho requisito" SAP Madrid de 25 de enero de 2012 (Sección 10) (ROJ: SAP M 1922/2012), FJ 16. También sobre el incumplimiento de un requerimiento previo de pago antes de incluir los datos en un fichero de morosos versa otra sentencia, en la que se vuelve a insistir en que la responsabilidad es objetiva según "entiende de forma casi unánime la doctrina […] dados los términos de redacción del artículo 23 de la Directiva 95/46/CE". Si bien se alude a que en autos ni obra ni consta este requerimiento, SAP Segovia de 25 de abril de 2002 (Sección 1) (ROJ: SAP SG 168/2002), FJ 1.

Si estamos ante una obligación de resultado (como el deber de secreto), ante la no producción del resultado deseado por el precepto (la revelación a un tercero de información), deberá establecerse que ha habido incumplimiento y esto supondrá una responsabilidad objetiva, pues no permitirá la prueba de la diligencia debida por parte del responsable.

Por último, hay que mencionar que cuando se trate de responsabilidad de Administraciones Públicas, en el caso de ficheros de titularidad pública, claramente se ha optado por una responsabilidad objetiva[1226], lo que, sin duda, contrasta con la carencia de sanciones económicas en el ámbito sancionador administrativo[1227]. De esta forma, las Administraciones deberían reparar los daños pero no estarán sujetas al régimen punitivo.

vi. Responsabilidad por hecho ajeno

Al igual que se señalaba respecto a la Directiva 95/46/CE, el artículo 19 LOPD tampoco hace referencia al supuesto en el que la acción u omisión la realice una persona empleada del responsable o del encargado del tratamiento. Por tanto, sería aplicable el régimen del artículo 1903 CC relativo a la responsabilidad por los dependientes. De nuevo, pese a que el artículo 1903 CC remite para estos supuestos a lo indicado por el artículo 1902 CC y, por tanto, parecería que de nuevo se trataría de una responsabilidad subjetiva, también la jurisprudencia lo entiende como un supuesto de responsabilidad objetiva[1228].

[1226] Especialmente crítico con esta responsabilidad objetiva es F. PANTALEÓN PRIETO, "Cómo repensar la responsabilidad civil extracontractual (También la de las Administraciones Públicas)", R. DE ÁNGEL YÁGÜEZ, M. YZQUIERDO TOLSADA (Coord.), VVAA, *Estudios de responsabilidad civil en homenaje al profesor Roberto López Cabana*, Dykinson, Madrid, 2001, págs. 205 a 216.

[1227] Como indica ORDÓÑEZ SOLÍS la acción indemnizatoria adquiere mayor relevancia cuando se interpone contra las Administraciones Públicas en la medida en que no se ha previsto un régimen de sanciones equivalente al que se puede imponer al sector privado. D. ORDÓÑEZ SOLÍS, *Privacidad y protección judicial de los datos personales, op. cit.*, pág. 217.

[1228] Así PEÑA LÓPEZ indica que, pese a que de la lectura superficial de las sentencias del TS parecería que se parte de los actos propios del principal para ver si se puede apreciar la culpa del mismo, se termina por concluir que la conducta del principal no tiene trascendencia. Por tanto, en lugar de una responsabilidad por culpa se establece una responsabilidad vicaria, en la que es suficiente que exista una relación de dependencia entre el dependiente que ocasiona el daño y el principal, sin que tenga importancia, la conducta del principal. Así, este autor manifiesta que, si bien la interpretación jurisprudencial no coincide con la letra de la ley, el régimen de responsabilidad que establece es similar al que establecen los ordenamientos de nuestro entorno. F. PEÑA LÓPEZ, "Capítulo II. De las obligaciones que nacen de culpa o negligencia", R. BERCOVITZ RODRÍGUEZ-CANO, VVAA *Comentarios al Código Civil, Tomo IX, op.cit.*, pág. 13.008. Asimismo, O'CALLAGHAN considera que la responsabilidad que contempla el artículo 1903 Cc por

GRIMALT SERVERA consideraba que, al vincularse el deber de reparar con el incumplimiento de lo establecido en la ley, además de suponer la responsabilidad objetiva para el caso de que sea el responsable del fichero quien directamente sea el causante de este incumplimiento, también debía incluir los supuestos en los que fuera un dependiente quien ocasionara ese incumplimiento. De esta forma, equiparaba este supuesto al establecido en el artículo 1910 CC que establece claramente una responsabilidad objetiva del cabeza de familia respecto a los hechos ocurridos en su casa[1229]. Según el autor, el legislador pretendía "concentrar toda la responsabilidad en el responsable del fichero, pues se trata de un sujeto determinado y conocido".

Además en los proyectos que, a nivel europeo, se desarrollan actualmente para aproximar las legislaciones civiles, se destaca la configuración de la responsabilidad de las empresas mediante la atribución automática de las acciones u omisiones realizadas por sus dependientes. De esta forma se atribuye la responsabilidad a la actividad organizativa en sí misma considerada, de forma que la empresa resulta obligada a reparar el daño cuando ha sido ocasionado por alguno de los miembros de la organización[1230].

En algunas de las leyes nacionales de los Estados miembros de la UE se hace referencia a este supuesto. Así, en la Ley austríaca, además de contemplar la posibilidad de que el interesado solicite una indemnización, de acuerdo con el derecho civil, al responsable o al encargado del tratamiento, si fueran estos culpables de usar los datos vulnerando la ley, también se añade que el responsable y el encargado responderán de los daños causados por sus empleados. En este sentido, se especifica que no serán

---

hecho ajeno referida al empresario respecto a los daños causados por los empleados en relación de subordinación o dependencia es objetiva, directa, solidaria incluso cuando no se conociera quién ha sido el empleado que ha causado el daño. X. O'CALLAGHAN MUÑOZ, "La responsabilidad objetiva" ", J.A. MORENO MARTÍNEZ (Coord.), VVAA, *La responsabilidad civil y su problemática actual*, *op. cit.*, pág. 812.

[1229] Ya se indicaba que el autor argumentaba en apoyo del criterio de la responsabilidad objetiva que en los debates parlamentarios de elaboración de la LORTAD incluso se había mencionado este supuesto concreto del artículo 1910 Cc para rechazar una enmienda al artículo 17.1 LORTAD. P. GRIMALT SERVERA *La responsabilidad civil en el tratamiento automatizado de datos personales, op.cit.* págs. 229 a 231. BUSTO considera que en estos supuestos resultaría de aplicación el artículo 1903.4 Cc, sin perjuicio de la posibilidad de interponer acción de repetición *ex* artículo 1904 Cc. J.M. BUSTO LAGO, "La responsabilidad de los responsables de ficheros de datos personales y de los encargados de su tratamiento", *Revista Aranzadi Civil-Mercantil, op. cit.* pág. 7.

[1230] Estas propuestas son los PETL (*Principles of European Tort Law*) y el DCFR (*Draft Common Frame of Reference*) y esta regulación en concreto es encuentra en PETL 6:102 y DCFR VI.3:201.

responsables si pudieran probar que las causas que provocaron el daño no se les pueden atribuir a ellos ni a sus empleados (Parágrafo 33 Ley austríaca)[1231].

En el caso del encargado del tratamiento, además de que deberá indemnizar por aquellos incumplimientos que se le puedan atribuir, cabe plantearse si también se podría ir contra el responsable que lo hubiera contratado por una culpa *in eligendo* o *in vigilando* (ex art. 1903 Cc). De las obligaciones que la LOPD establece para el responsable queda patente que la respuesta a esta cuestión tiene que ser afirmativa, ya que se le exige expresamente la obligación de velar porque el encargado reúna las garantías para cumplir con el RLOPD (art. 20.2 RLOPD)[1232].

2.4.2. Responsabilidad penal

a. La protección penal del derecho a la protección de datos

En el ordenamiento jurídico español la responsabilidad penal se establece de forma separada, en el Código Penal[1233]. Debido a ser un derecho de reconocimiento reciente, se ha planteado si el derecho a la protección de datos era merecedor de una protección penal, que sólo puede operar cuando la protección extrapenal sea insuficiente[1234]. Una vez superado este debate para entender que este derecho también debía recibir esta protección penal, se ha criticado la rúbrica del Título X, en el que se

[1231] También cabe mencionar la Ley húngara que establece que el responsable del tratamiento se hará cargo de la indemnización también en el caso de que el daño lo hubiera generado el encargado del tratamiento (Sección 23 Ley húngara).
[1232] Se ha admitido por la jurisprudencia la aplicación del artículo 1903 Cc en casos de responsabilidad por daños ocasionados por una empresa autónoma contratada cuando se reserve el comitente la vigilancia o, aunque no hiciera tal reserva, cuando pueda identificarse a su cargo un deber de cuidado, del que no pueda liberarse delegándolo en el contratante. E. GÓMEZ CALLE, "Capítulo VI. Los sujetos de la responsabilidad civil. La responsabilidad por hecho ajeno", L.F. REGLERO CAMPOS (Coord.), VVAA, *Tratado de responsabilidad civil, Tomo I Parte General, op. cit.*, págs. 1.045 a 1.055.
[1233] Como se ha visto esto no sucede en otros ordenamientos que incluye infracciones penales en las leyes de protección de datos. De hecho, MORALES opina que hubiera sido "más cauteloso" incluir tipos penales en la LOPD, con el fin de facilitar una mejor comprensión de los conceptos empleados y una armonización de los mismos. F. MORALES PRATS, "Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", G. QUINTERO OLIVARES (Dir.), F. MORALES PRATS (Coord.), VVAA, *Comentarios a la Parte Especial del Derecho Penal*, 8ª Ed., Aranzadi, Cizur Menor (Navarra), 2009, pág. 421.
[1234] J. GÓMEZ NAVAJAS, *La protección de los datos personales: un análisis desde la perspectiva del derecho penal*, Aranzadi, Cizur Menor (Navarra), 2005, pág. 79.

incardina (delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio), ya que no refleja esta inclusión del derecho a la protección de datos[1235].

Sin pretender realizar un estudio detallado de los preceptos penales, me quiero referir a algunos aspectos especialmente relacionados con la protección de datos y el responsable.

Se ha considerado que el tipo básico contenido en el artículo 197 CP es el relativo al apoderamiento de papeles, cartas, mensajes de correo electrónico, documentos o efectos personales con intención de descubrir secretos o vulnerar la intimidad (art. 197.1 CP)[1236]. También se tipifica la interceptación de las telecomunicaciones o la utilización de artificios técnicos con la misma finalidad de acceder a los secretos o vulnerar la intimidad de otro.

Sin embargo, el tipo que se ha considerado dirigido a proteger el derecho de protección de datos es el referido a quien, sin autorización, se apodere, utilice o modifique en perjuicio de tercero, datos reservados de carácter personal o familiar o a quien acceda y los altere en perjuicio del titular o de un tercero (art. 197.2 CP)[1237].

Algunos aspectos del tipo han tenido que ser delimitados por la doctrina y la jurisprudencia. En este sentido, el alcance del delito es respecto a aquellos datos "ya registrados", por lo que no intervendría el derecho penal en el momento previo al registro, es decir, en la recogida de datos[1238].

[1235] Sugiere GÓMEZ NAVAJAS que debería cambiarse para llamarse "Delitos contra la intimidad, la libertad informática y la inviolabilidad del domicilio" aunque no cree que deba modificarse la ubicación sistemática debido a su conexión con el derecho a la intimidad. *Ibídem*, pág. 83.

[1236] F. MORALES PRATS, "Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", G. QUINTERO OLIVARES (Dir.), F. MORALES PRATS (Coord.), VVAA, *Comentarios a la Parte Especial del Derecho Penal*, *op. cit.*, pág. 408.

[1237] *Ibídem*, págs. 416 a 419. Asimismo, se pueden citar algunas sentencias del Tribunal Supremo que, no obstante, precisar que se lo que se protege es la libertad informática entendida como derecho del ciudadano a controlar la información personal y familiar que se encuentra recogida en ficheros de datos, indica que constituye una dimensión positiva de la intimidad que es el bien jurídico protegido, STS de 30 de diciembre de 2009 (Sala 2ª) (ROJ: STS 8457/2009), FJ 6, STS de 17 de junio de 2014 (Sala 2ª) (ROJ: STS 3545/2014), FJ 5.

[1238] F. MORALES PRATS, "Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", G. QUINTERO OLIVARES (Dir.), F. MORALES PRATS (Coord.), VVAA, *Comentarios a la Parte Especial del Derecho Penal*, *op. cit.*, pág. 422.

Otra cuestión suscitada ha sido el significado del término "reservados", ya que no está en consonancia con el ámbito de aplicación de la LOPD y parece más una reminiscencia del derecho a la intimidad. La LOPD no diferencia entre los datos personales, excepto en lo que se refiere a los datos especialmente protegidos. Sin embargo, precisamente se establece como tipo agravado la protección de estos datos especialmente protegidos (art. 197.5 CP), lo que implica que "reservados" no puede querer decir "especialmente protegidos". Finalmente, se ha optado por entender que este concepto normativo debe entenderse referido a los datos que no son susceptibles de ser conocidos por cualquiera, lo que se conecta con el hecho de que quien accede a los datos o los utiliza lo hace "sin autorización"[1239].

Otro elemento que ha dado dificultades de interpretación ha sido determinar que significa que la conducta se realice "en perjuicio de tercero". Lo que se cuestionaba era si esta expresión debía considerarse un elemento subjetivo del injusto o si debía exigirse la producción del resultado. La relevancia constitucional del bien jurídico protegido ha hecho que se opte por no exigir resultado lesivo y que se trate como un delito de peligro[1240].

Cuando se indica que la conducta será "en perjuicio de tercero", la expresión "tercero" parece referirse al titular de los datos. Sin embargo, en la segunda parte del tipo se hace referencia a quien acceda o altere o utilice los datos "en perjuicio del titular o de un tercero". Por tanto, este tercero parece que sería un sujeto diferente al titular de los datos. Se ha interpretado, no obstante, que el concepto de "tercero" en todo caso debe incluir al titular de los datos y que también podría referirse a quienes custodian y garantizan datos de los titulares, es decir, a los responsables[1241].

Además se establecen tipos agravados si los datos o hechos descubiertos se difunden, revelan o ceden a terceros, y también en función de los sujetos que los cometan.

[1239] STS de 17 de junio de 2014 (Sala 2ª) (ROJ: STS 3545/2014) FJ 5 y STS de 30 de diciembre de 2009 (Sala 2ª) (ROJ: STS 8457/2009), FJ 9.
[1240] STS de 17 de junio de 2014 (Sala 2ª) (ROJ: STS 3545/2014), FJ 7.
[1241] MORALES PRATS así lo interpreta y cita, como ejemplo, la SAP Valladolid de 14 de julio de 1998 (Sección 2) (ROJ: SAP VA 1374/1998), que consideró como agraviada del delito analizado a una asociación de discapacitados, de cuyo fichero informático fueron sustraídos datos de sus afiliados. F. MORALES PRATS, "Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", G. QUINTERO OLIVARES (Dir.), F. MORALES PRATS (Coord.), VVAA, *Comentarios a la Parte Especial del Derecho Penal*, *op. cit.*, pág. 426.

En este último caso, se encuentra la autoridad o funcionario público (art. 198 CP)[1242], quién revelara secretos de los que tenga conocimiento por razón de su oficio o sus relaciones laborales o el profesional que incumpla su obligación de sigilo o reserva, al divulgar secretos (art. 199 CP)[1243]. Finalmente también se incluyen, entre los tipos agravados, los hechos mencionados en los apartados 1 y 2 del artículo 197 CP, que cometan "las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros" (art. 197.4.a CP).

En definitiva se daría cabida a aquellos sujetos que pueden acceder a los datos personales en función de su actividad. A diferencia de la LOPD, en el ámbito penal se castiga a las personas concretas que, en el ámbito de las empresas o administraciones públicas, puedan divulgar datos a los que accedan en principio lícitamente.

Respecto al último tipo mencionado hay que decir que, de nuevo, encontramos un ejemplo de la debilidad de la dualidad de los conceptos de responsable del tratamiento y responsable del fichero, ya que, en este precepto sólo se alude claramente a responsables del fichero, por lo que, parece que no podría aplicarse a los responsables del tratamiento. No obstante, como para interpretar el concepto de responsable debe acudirse al concepto de responsable de la LOPD podría suplirse este defecto con una interpretación acorde a este concepto que integra ambas figuras[1244]. De igual modo, debe interpretarse que "personas encargadas" responde al concepto de encargado del tratamiento[1245].

[1242] Hay que tener en cuenta que las autoridades y funcionarios públicos que revelen secretos también son sancionados con el artículo 417 CP. El Tribunal Supremo, no obstante, ha diferenciado ambos preceptos (417 y 198 CP) porque en el caso del 198 CP además del deber de secreto se infringe otro deber, ya que se apodera de datos que no debería conocer de acuerdo con sus funciones y en cambio en el 417 los datos que revela los obtiene en virtud de su cargo. Es decir en el caso del 198 CP el funcionario puede acceder a datos pero que no precisa para el ejercicio de sus funciones (por ejemplo porque no están relacionados con ninguno de los expedientes que gestiona). Por eso, este artículo contiene penas mayores que el 417 CP. STS de 17 de junio de 2014 (Sala 2ª) (ROJ: STS 3545/2014), FJ 4.

[1243] Responde este precepto al castigo de lo quienes se conocen como confidentes necesarios y responden a la infracción del deber de secreto establecido en el artículo 10 LOPD. STS de 9 de diciembre de 2010 (Sala 2ª) (ROJ: STS 7064/2010), FJ 1.

[1244] MORALES define el marco legal extrapenal informador de los elementos normativos del tipo con el Convenio 108, la Directiva 95/46/CE y la LOPD Asimismo, hay que tener en cuenta el régimen de infracciones administrativas de la LOPD para evitar el solapamiento entre la tutela penal y el régimen sancionador. F. MORALES PRATS, "Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", G. QUINTERO OLIVARES (Dir.), F. MORALES PRATS (Coord.), VVAA, *Comentarios a la Parte Especial del Derecho Penal, op. cit.*, pág. 420.

[1245] *Ibídem*, pág. 431.

Algún autor entiende que el fundamento de este tipo agravado hay que buscarlo en el principio de corresponsabilidad de los responsables del fichero junto a la AEPD[1246]. Esta posición de los responsables como garantes del derecho a la protección de datos de los titulares de estos datos, se puede completar con la aproximación a la responsabilidad penal de la persona jurídica que también se establece para los delitos comentados[1247]. Como se verá, existe una tendencia que se extiende a todas las ramas del derecho que nos lleva, en cierto modo, a "motivar" a los entes colectivos para que cumplan las normas. En el caso del derecho penal, mediante las últimas reformas se ha dado un gran paso en este sentido, como veremos a continuación.

b. La responsabilidad penal de la persona jurídica

Respecto a la determinación del sujeto responsable penalmente, es interesante hacer mención a cómo ha quedado configurada la responsabilidad de las personas jurídicas con las reformas realizadas en el 2010[1248] y en el 2015[1249] del Código Penal. Las reformas del Código penal respondían a una demanda suscitada por algunas normas internacionales[1250]. Estas modificaciones no estuvieron exentas de polémica, ya que quebraban la idea tradicional de ligar la responsabilidad penal a una persona física[1251].

Estas reformas reflejan las nuevas tendencias en la configuración de la atribución de responsabilidad a entes colectivos. Entre estas tendencias figuraba la autorregulación

[1246] MORALES entiende que este principio de corresponsabilidad se refleja en la elaboración de códigos tipo en los que los responsables fijen el régimen de funcionamiento y las medidas de seguridad de los tratamientos de datos. *Ibídem*, págs. 419 y 431.

[1247] Como indica GÓMEZ NAVAJAS, el ámbito de la delincuencia informática es uno de los ámbitos en los que con mayor claridad se aprecia la necesidad de articular vías para exigir la responsabilidad de las personas jurídicas. J. GÓMEZ NAVAJAS, *La protección de los datos personales: un análisis desde la perspectiva del derecho penal*, *op. cit.*, pág. 154.

[1248] Esta modificación se realizó por Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (BOE núm. 152 de 23.6.2010), que entró en vigor el 23 de diciembre de 2010 y consistió principalmente en la inclusión de un nuevo artículo 31 bis.

[1249] Reforma introducida por la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (BOE núm. 77 de 31.3.2015), que entró en vigor el 1 de julio de 2015.

[1250] Así, en el preámbulo de la Ley Orgánica 5/2010, antes mencionada, se hace referencia en su apartado VII a la razón de incluir esta regulación de la responsabilidad penal de las personas jurídicas, que no es otra que dar respuesta a los numerosos instrumentos jurídicos internacionales que lo demandan. Uno de estos instrumentos fue el Convenio de cibercriminalidad, convenio internacional cuya regulación se recogió en la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, decisión que se cumplió con la reforma de 2010.

[1251] No fue, por ejemplo, hasta la aprobación de la Ley 37/2011, de 10 de octubre, de medidas de agilización procesal, BOE de 11.10.2011, cuando se introdujeron algunas medidas para dar un estatuto procesal a la persona jurídica en el marco de los procedimientos penales.

que pretendía ser una vía para completar la acción del derecho positivo. Sin embargo, esta vía no ha sido suficiente en un contexto tan complejo como el actual. La complejidad reside, no sólo en la organización interna de las empresas[1252] sino en la multitud de normas que deben cumplir de diferentes ámbitos.

A estos aspectos, hay que añadir la tradición del sistema jurídico continental, que se ha orientado a la elaboración de normas, sin tener en cuenta la posterior aplicación de las mismas a las organizaciones[1253]. Consecuentemente, estas organizaciones se han enfrentado a una enorme complejidad normativa sin poseer ni la cultura ni la capacitación para poder cumplirla.

No obstante, las grandes empresas han implantado sistemas autorregulatorios para cumplir con obligaciones, provenientes de países como EEUU, de acuerdo con estándares creados para ello[1254]. Hay que tener en cuenta que pese al carácter individualista del *Common Law* fue éste el que originó la responsabilidad penal de la persona jurídica y los programas de cumplimiento[1255]. Este esquema fundamentado en obligaciones legales que se deben integrar en la organización interna de las entidades obligadas, mediante sistemas de autorregulación se adopta progresivamente en el derecho positivo continental. Para reforzar este sistema, se introduce la obligación de autorregularse en las leyes y se

[1252] M. BAJO FERNÁNDEZ, B.J. FEIJOO SÁNCHEZ, C. GÓMEZ-JARA DÍEZ, *Tratado de responsabilidad penal de las personas jurídicas*, Aranzadi, Cizur Menor (Navarra), 2012, pág. 111.

[1253] A diferencia del sistema jurídico anglosajón en el que se ha incentivado, en un enfoque más pragmático, la autorregulación y la aplicación práctica de las obligaciones legales.

[1254] Como ejemplo puede mencionarse la ley estadounidense *Foreign Corrupt Practices Act* (FCPA) de 1977 que pretende luchar contra la corrupción y que tiene alcance extraterritorial. Ver http://www.sec.gov/spotlight/fcpa.shtml (fecha consulta: 13.7.2015).

[1255] No obstante, también había reticencia a aceptar la responsabilidad de la persona jurídica, lo que se ilustra con la cita del *Lord Chancellor* Edward Thurlow que, a finales del siglo XVIII afirmó que las personas jurídicas "no tienen ningún alma a la que reprochar, ningún cuerpo que patear" (*no soul to be damned, and no body to be kicked*) y no fue hasta 1850 cuando la jurisprudencia la aceptó con el caso ante el Tribunal Supremo *New York Central & Hudson River Railroad v. United States.* A principios de los años ochenta los Estados federados y el Estado federal aprobaron leyes que exigían que el condenado cumpliera un porcentaje mínimo de la condena antes de ser liberado y se crearon las "*Sentencing Commissions*" encargadas de reformar el sistema de determinación de la pena. Para ello elaboraron unas directrices para la determinación individual de la pena (*Sentencing guidelines*) que además se acompañaron de extensos comentarios oficiales (*Manuals*). Las directrices para las personas físicas entraron en vigor el 1 de noviembre de 1987 y las de personas jurídicas (*Organizational Guidelines* o *Chapter eight*) el 1 de noviembre de 1991. Son estas directrices las que introducen posibles incentivos a empresas que mantengan mecanismos internos de prevención, detección y denuncia de conductas delictivas. I. ORTIZ DE URBINA GIMENO, "Responsabilidad penal de las personas jurídicas: *the american way*", S. MIR PUIG, M. CORCOY BIDASOLO, V. GÓMEZ MARTÍN (Dir.), VVAA, *Responsabilidad de la empresa y compliance. Programas de prevención, detección y reacción penal*, Edisofer, Madrid, 2014, págs. 37 a 52.

incluyen los aspectos básicos que deberán adoptarse a nivel formal para asegurar esa organización responsable.

Por tanto, el Estado, especialmente en el sistema continental, acude a una autorregulación regulada, de forma que el derecho de autorregulación se acompañe del deber de hacer frente a las consecuencias de ejercer esta capacidad de autorregulación[1256]. La persona jurídica adquiere, por tanto, una posición de garante sobre su propio ámbito organizativo que legitima que se pueda responsabilizar de las consecuencias del ejercicio de esta libertad autoorganizativa[1257].

Con la reforma de 2010 se estableció la responsabilidad penal de las personas jurídicas cuando sus representantes o administradores de hecho o de derecho cometieran algún delito en nombre o por cuenta de las mismas y en su provecho (art. 31.1 bis CP del texto reformado en el 2010). Asimismo, las personas jurídicas también serían responsables de los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en provecho de las mismas, por quienes estuvieran sometidos a la autoridad de las personas indicadas anteriormente, al considerarse que habrían cometido estos hechos por no haberse ejercido sobre ellos el debido control.

Esta regulación dio lugar a algunas dudas sobre el régimen de responsabilidad elegido por el legislador. Quienes se resistían al cambio de paradigma mantuvieron que la responsabilidad de la persona jurídica se había establecido mediante un modelo de heterorresponsabilidad o vicarial[1258]. De esta forma, se argumentaba que la persona

[1256] C. GÓMEZ-JARA DÍEZ, "Capítulo V Fundamentos de la responsabilidad penal de las personas jurídicas", M. BAJO FERNÁNDEZ, B.J. FEIJOO SÁNCHEZ, C. GÓMEZ-JARA DÍEZ, *Tratado de responsabilidad penal de las personas jurídicas, op. cit.,* pág. 113.
[1257] *Ibídem,* págs. 121, 131 a 133.
[1258] Esta fue la clara postura de la Fiscalía General del Estado que consideraba que este sistema no obligaba a generar así una nueva teoría general del delito, "empresa tan solo esbozada tímidamente por algunos autores y que, a día de hoy, se antoja de resultados francamente inciertos". Circular 1/2011 relativa a la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por la Ley Orgánica 5/2010, pág. 30. También es la tesis defendida por MIR PUIG que considera que la letra de este artículo 31 bis CP era clara al establecer la responsabilidad penal de la persona jurídica en virtud de los delitos cometidos por las personas físicas señaladas. Con el fin de que las penas establecidas para las personas jurídicas por estos hechos cometidos por otro no infrinjan el principio de culpabilidad, este autor defiende que son distintas de las establecidas para las personas físicas. Las penas de las personas jurídicas se aproximan más a las sanciones administrativas y a las medidas de seguridad y las consecuencias accesorias, ya que son básicamente preventivas y económicas. Así, las penas de la persona jurídica no tendrían el mismo carácter de reproche ético-jurídico que las penas de las personas físicas. Las penas previstas para las personas jurídicas están en el artículo 33.7 CP, introducido por la Ley Orgánica 5/2010 y que no ha sufrido cambios con la Ley Orgánica 1/2015. S. MIR PUIG, "Las nuevas "penas" para personas

jurídica era responsable por los delitos cometidos por las personas físicas que actuaran en su seno, por lo que se trataría, en realidad, de una transferencia de responsabilidad y no de una responsabilidad autónoma de la persona jurídica.

Sin embargo, parte de la doctrina defendió el establecimiento de un régimen de autorresponsabilidad de la persona jurídica[1259]. En defensa de esta postura se acudía a una parte del precepto que especificaba que la responsabilidad penal de la persona jurídica se podía establecer independientemente de que se pudiera o no individualizar la responsabilidad penal de la persona física que realizara la conducta infractora (art. 31 bis.2 CP del texto reformado en 2010). De esta forma, se afirmaba que esta previsión permitía una atribución autónoma de responsabilidad que se desligaba de la conducta de la persona física.

Otro rasgo que inducía a los autores a defender el régimen de autorresponsabilidad era el control que se exigía por parte de los gestores de la persona jurídica a sus subordinados. Así, consideraban que era presupuesto necesario para entrar a examinar la responsabilidad de la persona jurídica que las personas físicas vinculadas a la misma cometieran un delito, pero la persona jurídica no respondería por estos hechos. La persona jurídica respondería por su propio injusto que consistiría en un defecto de organización y en función de su propia culpabilidad[1260].

Así, con la reforma de 2015 se desarrolla precisamente el aspecto relativo al debido control que debe existir en el seno de la persona jurídica que asegure que no

---

jurídicas: una clase de "penas" sin culpabilidad", S. MIR PUIG, M. CORCOY BIDASOLO, V. GÓMEZ MARTÍN (Dir.), VVAA, *Responsabilidad de la empresa y compliance. Programas de prevención, detección y reacción penal*, *op. cit.*, págs. 3 a 5, 8.

[1259] En este sentido M. BAJO FERNÁNDEZ, B.J. FEIJOO SÁNCHEZ, C. GÓMEZ-JARA DÍEZ, *Tratado de responsabilidad penal de las personas jurídicas*, *op. cit.*

[1260] Esta es la postura de GÓMEZ-JARA DÍEZ, que entiende que, al igual que la persona física tiene la capacidad de acción que posibilita su responsabilidad, la persona jurídica tiene capacidad de organización que también debe servir para atribuirle responsabilidad. Además de entender que el defecto de organización es lo que conforma el injusto, respecto a la culpabilidad que tantas dificultades interpretativas suscitó respecto a la persona jurídica, entiende que debe referirse a la cultura empresarial de incumplimiento de la legalidad. Así una persona jurídica será culpable si ha desarrollado esta cultura del incumplimiento. C. GÓMEZ-JARA DÍEZ, "Capítulo V Fundamentos de la responsabilidad penal de las personas jurídicas", M. BAJO FERNÁNDEZ, B.J. FEIJOO SÁNCHEZ, C. GÓMEZ-JARA DÍEZ, *Tratado de responsabilidad penal de las personas jurídicas*, *op. cit.*, pág. 109.

incurrirá en este defecto de organización. Con los cambios introducidos parece que se pretenden resolver las dudas de interpretación para alejarse del régimen vicarial[1261].

El nuevo artículo 31 bis CP mantiene el presupuesto previo necesario para atribuir la responsabilidad a la persona jurídica consistente en la comisión de un delito por las personas vinculadas a la misma[1262]. Sin embargo, se establece la exoneración de la persona jurídica en caso de que haya adoptado modelos de organización y gestión que incluyan medidas de vigilancia y control para prevenir la comisión de los delitos[1263]. Estos modelos son los conocidos como programas de *compliance* o de cumplimiento normativo[1264].

Como puede apreciarse, queda patente lo similar de esta aproximación por parte del legislador penal a la que otras normativas han adoptado, entre las que está la normativa de protección de datos o la que regula la prevención de riesgos laborales o la protección del medio ambiente. En todas ellas, se traspasa a las organizaciones esta

[1261] Así, el preámbulo de la Ley Orgánica 1/2015 explica que se pretende delimitar el contenido del "debido control" cuyo quebrantamiento permite fundamentar la responsabilidad penal y, en concreto, se quiere poner fin a las dudas interpretativas de la anterior regulación, al considerarse que era un régimen de responsabilidad vicarial.

[1262] Por tanto, pese a lo establecido en el preámbulo de la Ley Orgánica 1/2015, quienes, como MIR PUIG han fundamentado que el régimen de responsabilidad era el vicarial, en función de este presupuesto previo podrán mantener esta argumentación. Así se establece que las personas jurídicas serán responsables penalmente "de los delitos cometidos en nombre o por cuenta de las mismas, y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma" y también "de los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por haberse incumplido gravemente por aquéllos los deberes de supervisión, vigilancia y control de su actividad atendidas las concretas circunstancias del caso" (art. 31 bis.1, apdos a y b CP).

[1263] De esta forma, en el caso de los delitos cometidos por el primer colectivo referido a los representantes, autorizados o gestores se exige para exonerar a la persona jurídica que el órgano de administración haya adoptado estos modelos antes de la comisión del delito; que la supervisión de los mismos se haya confiado a un órgano autónomo; que los autores del delito lo hayan cometido eludiendo fraudulentamente el modelo y que no se haya producido una omisión o un ejercicio insuficiente de sus funciones de supervisión, vigilancia y control por parte del órgano autónomo (art. 31 bis.2 CP). En el caso de los delitos cometidos por las personas subordinadas, la persona jurídica quedará exonerada si ha adoptado y ejecutado eficazmente un modelo de organización y gestión adecuada para prevenir delitos de la naturaleza del cometido o para reducir de forma significativa su comisión (art. 31 bis.4 CP).

[1264] También se han desarrollado los requisitos que estos modelos deben cumplir: identificar las actividades en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos; establecer los protocolos o procedimientos que concreten el proceso de formación de la voluntad de la persona jurídica; disponer de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los delitos; imponer la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el modelo; establecer un sistema disciplinario y realizar una verificación periódica del modelo y su modificación si se producen infracciones relevantes o se producen cambios en la organización, en la estructura del control o en la actividad desarrollada (art. 31 bis.5 CP).

obligación de aplicar programas de cumplimiento normativo que persigan el aseguramiento de los objetivos de estas normas[1265]. Son estas organizaciones las que podrán erigirse en garantes de estos objetivos, las que más eficazmente podrán instaurar los mecanismos para prevenir el incumplimiento.

Con estos programas de cumplimiento lo que se pretende es hacer de las empresas "ciudadanos" respetuosos y cumplidores de la legislación que les afecta[1266]. El buen gobierno, la reputación corporativa y la transparencia se convierten en valores que deben regir la actividad de las organizaciones, tanto del sector público como privado, ante unos ciudadanos más críticos con las malas praxis.

En el otro lado de la balanza, hay que tener en cuenta que la instauración de estos programas conlleva un mayor riesgo de vulneración de los derechos de las personas sometidas a los mismos, especialmente de los empleados de la organización. Entre estos derechos que se encontrarán en peligro estará el de protección de datos pero también otros como el de intimidad, el de secreto de comunicaciones o el de libertad de expresión[1267]. Tanto en el derecho privado, como en el derecho público, asistimos al necesario equilibrio entre la capacidad de control por parte de las organizaciones y la posible vulneración de derechos como consecuencia de estos controles.

[1265] Así ya se ha examinado que el RLOPD obliga a la adopción de un documento de seguridad o la legislación de prevención de riesgos laborales obliga a la adopción de planes de prevención de riesgos (art. 16 Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales, BOE 10.11.1995).

[1266] A.D. BLUMENBERG, B. GARCÍA-MORENO, "Retos prácticos de la implementación de programas de cumplimiento normativo", S. MIR PUIG, M. CORCOY BIDASOLO, V. GÓMEZ MARTÍN (Dir.), VVAA, *Responsabilidad de la empresa y compliance. Programas de prevención, detección y reacción penal*, *op. cit.*, pág. 284.

[1267] Respecto al derecho de protección de datos se puede ejemplificar con los aspectos que han planteado los sistemas de denuncias internos, uno de los elementos habituales de los programas de *compliance*. Ver Dictamen 1/2006 relativo a la aplicación de las normas sobre protección de datos de la UE a los sistemas internos de denuncia de irregularidades en los ámbitos de la contabilidad, controles de auditoría internos, cuestiones de auditoría, lucha contra la corrupción y delitos financieros y bancarios, 195/06/ES WP 117, 1.2.2006, Grupo de trabajo Artículo 29 sobre la protección de datos y el Informe 128/2007 de la AEPD sobre creación de sistemas de denuncias internas en las empresas (mecanismos de "*whistleblowing*").

2.5. Régimen sancionador administrativo

2.5.1. La determinación del sujeto infractor en las legislaciones nacionales europeas

La LOPD establece claramente que ambas figuras, el responsable y el encargado, estarán sujetas al régimen sancionador establecido en la ley (art. 43.1 LOPD). Sin embargo, en muchas de las leyes nacionales que transponen la Directiva 95/46/CE no se da esta asignación de sanciones a responsables y encargados tan claramente.

Un grupo de estas leyes establece de forma neutra los sujetos infractores, como la Ley alemana que, para definir a estos sujetos utiliza la palabra "cualquiera"[1268]. En estos casos, la asignación de las infracciones se verá condicionada a la mayor o menor claridad con la que se adjudiquen las obligaciones en el articulado de las leyes. La Ley luxemburguesa establece el cuadro sancionador también de forma neutra, pero el establecimiento de las sanciones se realiza en cada uno de los artículos que regulan la obligación en concreto, por lo que, en este caso, el sujeto infractor viene claramente delimitado por quien es el sujeto obligado a cumplir cada precepto.

En otras leyes tampoco se imponen sanciones al responsable porque se busca castigar a la persona que realice la conducta infractora, de forma que puede perseguirse incluso a los empleados o personas autorizadas por el responsable[1269]. Cuando estas

[1268] "An administrative offence shall be deemed to have been committed by anyone who, whether intentionally or through negligence[…]" Artículo 43 Ley alemana que se titula: "Administrative offences" (subrayado de la autora). Se incluirían en este grupo las siguientes leyes: artículos 42 y 43 Ley estonia, artículo 48 Ley finlandesa, artículo 47 Ley maltesa, artículos 35 y siguientes Ley portuguesa, artículos 43 y siguientes Ley noruega. La Ley rumana también la incluiríamos a excepción de la infracción por tratamiento ilícito de los datos de una de las infracciones que asigna al responsable o su representante (artículos 31 y siguientes Ley rumana).

[1269] En la Ley eslovena no se indica expresamente que las sanciones se impongan al responsable de los datos sino a la persona jurídica, empresario autónomo o individuo que lleve a cabo la conducta infractora (art. 91 a 103 Ley eslovena). La Ley irlandesa considerará infractores a los empleados o agentes que actúen sin autorización del responsable o el encargado. De esta forma, no se sigue la sistemática de sancionar a estos sujetos por entender que, al actuar sin autorización, se convierten en responsables, sino que se les tipifica como sujetos infractores independientemente del rol atribuido. A lo largo de la Ley irlandesa se contempla la tipificación de conductas que serán susceptibles de condena. La ley se refiere al sujeto obligado de forma neutra como la persona que realice la conducta (*a person*). Por ejemplo, se establece que los datos que trate un encargado del tratamiento no podrán ser comunicados por él o por ninguno de sus empleados o agentes sin autorización previa del responsable por cuenta del que actúan. A este respecto se prevé que la persona que incumpla este precepto será considerado culpable de esta infracción, por lo que se refiere, tanto al encargado, como a sus empleados o agentes (artículo 21 Ley irlandesa). La Ley polaca establece, en esta misma línea, que si la inspección revela que una acción o fallo en las tareas que debía llevar a cabo el jefe de una unidad organizativa, sus empleados o cualquier otra persona física, que actuara

personas son jurídicas, algunas normas establecen reglas para establecer qué sujetos dentro de la persona jurídica deberán asumir la sanción[1270].

En algunas leyes, se imponen sanciones a figuras diferentes a la del responsable, como al representante del mismo[1271] o a quien se comunican los datos[1272]. Asimismo, también se asignan sanciones a otros sujetos que realizan conductas que son susceptibles de ser cometidas por sujetos diferentes al responsable[1273].

La falta de asignación clara de las infracciones al responsable o al encargado, también responde, en ocasiones, a la inclusión en el régimen sancionador de tipos penales. Esta tipificación se centra más en la infracción, en la conducta que es la que señala quien es el sujeto infractor, ya que, de nuevo, se persigue castigar al individuo que efectivamente ha realizado esta conducta[1274].

---

como responsable, pudiera considerarse una infracción, de acuerdo con lo que establece la ley, la autoridad de control lo pondrá en conocimiento del órgano competente para perseguirlo, entregando las evidencias de estas sospechas (art. 19 Ley polaca).

[1270] La Ley irlandesa contiene una disposición relativa a la responsabilidad de los directores y otros responsables de personas jurídicas. Cuando la infracción la haya cometido una persona jurídica y se pruebe que se ha cometido con el consentimiento o la connivencia o que sea atribuible a alguna negligencia de una persona que fuera director, gerente, secretario u otro cargo de la persona jurídica, o una persona que aparentemente hubiera actuado ostentando esa capacidad, esta persona, así como la persona jurídica, se considerarán responsables de la infracción. Si las actividades de la persona jurídica se gestionan por sus miembros esta previsión se aplicará con relación a los actos u omisiones de un miembro en conexión con sus funciones de gestión como si fuera un director o gerente de la sociedad (art. 29 Ley irlandesa). En la Ley chipriota en caso de que el responsable no sea una persona física, se considerará responsable respecto a las sanciones penales el representante de la persona jurídica o el jefe de la autoridad pública, servicio u organización, si esta persona lleva a cabo la administración o gestión (art. 26.5 Ley chipriota). También se pueden imponer sanciones económicas a los responsables de una persona jurídica en la Ley croata (art. 36 Ley croata).

[1271] La ley austríaca sanciona al representante del responsable cuando éste no resida en la UE y al operador designado en el supuesto de sistemas conjuntos de información (Parágrafos 6.3 y 50.1 Ley austríaca).

[1272] La Ley croata considera sujeto infractor, además del responsable y el encargado, al que denomina la ley *user*, que es el sujeto al que se comunican datos (art. 36 Ley croata).

[1273] Un ejemplo de este supuesto es la Ley belga, en la que la mayoría de las infracciones tipificadas tienen asociadas como sujetos que son potenciales infractores de las mismas al responsable del tratamiento, su representante en Bélgica, su encargado de la protección de datos o su mandatario. No obstante, en tres de las infracciones se establece un posible infractor neutro al que se refiere la ley como "*quiconque*", que se puede traducir como "el que" o "quien". Entre estos supuestos se incluye el de obstaculización a la autoridad de control belga, sus miembros o expertos respecto a su capacidad de verificar el cumplimiento de lo establecido en la ley. Los otros supuestos sancionan a quien obliga a una persona a darle los datos obtenidos del ejercicio del derecho de acceso o a dar su autorización al tratamiento de datos por medio de violencia, amenazas, regalos o promesas y también a quien haya transferido o dejado transferir datos personales a un país no miembro de la UE (apdos. 6, 12 y 13 art. 39 Ley belga). Respecto a esta obstaculización de la actividad de inspección de la autoridad de control, también la establece sin asignarla a responsable o encargado, el artículo 42.7 Ley búlgara y la Ley polaca que establece algunas infracciones que asigna al responsable pero en otras deja una asignación neutral, como la que se refiere a la obstrucción de las actividades de inspección (art. 54a Ley polaca).

[1274] Esto sucede respecto a la tipificación penal en la Ley alemana: "*Anyone who wilfully commits an offence*[…]" artículo 44 Ley alemana, que se titula: "*Criminal offences*" (subrayado de la autora). También

2.5.2. El régimen sancionador en la legislación española

a. Los sujetos infractores

Como ya se ha mencionado, los sujetos infractores aparentemente están bien definidos en la normativa española. Y es que la LOPD señala a los responsables de los ficheros y los encargados de los tratamientos como sujetos sancionables. Sin embargo, ya se abordó en este trabajo que pese a esta aparente claridad, también se ha dado cabida en el régimen sancionador a otra tipología de sujetos: los responsables del tratamiento[1275].

El cuadro sancionador (art. 44 LOPD) no especifica las infracciones que se atribuyen a los diferentes sujetos, por lo que habrá que acudir a las obligaciones que derivan en estas infracciones para ver a quien se atribuyen exactamente. Así, por ejemplo la infracción que se refiere a la no inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos (art. 44.2.b LOPD) sólo podrá ser cometida por el responsable del fichero. A excepción de esta obligación de notificación, el responsable del tratamiento tendrá las mismas obligaciones que el responsable del fichero.

Sin embargo, respecto al encargado del tratamiento es algo más complejo que un examen de las obligaciones que se le atribuyen. Esta complejidad se refleja en lo estipulado en la LOPD cuando prevé que "en el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente" (art. 12.4 LOPD).

Hay que tener en cuenta que la conversión del encargado en responsable debe conectarse con su finalidad que, como indican ambos preceptos, es la de que responda de

sucede en el artículo 70.1 Ley danesa, artículo 22 Ley griega, artículos 167 a 172 Ley italiana, artículos 25 y 26 Ley chipriota.

[1275] Ver Capítulo III y SSTS de 5 de junio de 2004 (Sala 3ª) (ROJ: STS 3896/2004), de 28 de febrero de 2005 (Sala 3ª) (ROJ: STS 1234/2005) y de 26 de abril de 2005 (Sala 3ª) (ROJ: STS 2570/2005).

las infracciones en que hubiera concurrido personalmente[1276]. Por tanto, la finalidad no es que se convierta en responsable sino que pueda ser sancionado si destina los datos a otra finalidad, los comunica o los utiliza incumpliendo las estipulaciones del contrato[1277].

La utilización del término "personalmente" ha planteado si cabía entender que, en caso de que el encargado destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato implicaba que se exoneraba al responsable[1278]. Sin embargo la Audiencia Nacional ha señalado que el hecho de que se establezca que "será considerado, también, responsable del tratamiento", este término "también" deja claro que no se establece allí un mecanismo de sustitución ni de derivación de responsabilidades, sino de agregación, pues el responsable del fichero no pierde su condición de tal ni queda exonerado de responsabilidad por el hecho de que al encargado del tratamiento que incumpla lo estipulado se le atribuya también la consideración de responsable del tratamiento[1279].

Se ha establecido una exclusión de responsabilidad para el encargado si lo que hace es comunicar datos a un tercero en virtud de una indicación expresa del responsable, por haberle encomendado a ese tercero un servicio (art. 20.3 RLOPD)[1280].

En este sentido, hay que indicar que en la legislación española no se ha previsto la vía de escape que se contemplaba en el artículo 16 Directiva 95/46/CE relativa al imperativo legal. Es decir, en nuestra normativa no se ha previsto como posible

[1276] J. RUBÍ NAVARRETE, "El encargado del tratamiento", A. PALOMAR OLMEDA, P. GONZÁLEZ ESPEJO (dirs.); C. ÁLVAREZ RIGAUDIAS (Coord.), VVAA, *Comentario al Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal: (aprobado por RD 1720/2007, de 21 de diciembre), op. cit.*, págs. 228 a 229.

[1277] Como indica RUBÍ NAVARRETE, al remitir el artículo 20.3 RLOPD específicamente en este caso al contrato al que se refiere el artículo 12.2 LOPD, lo que se quiere dejar claro es que, si bien en el contrato se podrán incluir previsiones muy diversas, sólo las que se refieran específicamente a la regulación de protección de datos serán las que se tendrán en cuenta a la hora de determinar la responsabilidad del encargado por incumplimiento. *Ibídem.*

[1278] M. VIZCAÍNO CALDERÓN, *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, pág. 182.

[1279] SAN de 17 de mayo de 2013 (Sala de lo contencioso-administrativo) (ROJ: SAN 2172/2013), FJ 3, que remite, a su vez, a las sentencias de 13 de abril de 2005 (Recurso nº 241/2003) y de 14 de marzo de 2007 (Recurso nº 280/2005).

[1280] Esta previsión es superflua, ya que si el encargado actúa en este sentido por seguir una indicación expresa del responsable, no hará más que cumplir con sus instrucciones. Su inclusión responde a que no se preveía en los contratos la posibilidad de que el encargado comunicara los datos a otro nuevo encargado de forma directa, si el responsable decidía sustituirlo. De esta manera se intenta facilitar el traspaso de datos entre prestadores de servicios, lo que es especialmente importante en el contexto digital, donde el traspaso informático es más fácil que lo hagan directamente los prestadores tecnológicos.

legitimación del tratamiento que realice el encargado o las personas bajo la autoridad del responsable o del encargado, que éste tratamiento responda al cumplimiento de un imperativo legal. No obstante, hay que interpretar que un encargado o cualquier sujeto que deba cumplir con una obligación legal de carácter imperativo que contradiga las instrucciones u omisión de las mismas por parte del responsable no podrá ser sancionado en virtud de este posible incumplimiento, ya que estará legitimado para tratar los datos en virtud de una ley, como permite el artículo 6 LOPD.

b. El procedimiento y el marco sancionador reformado

El procedimiento sancionador en materia de protección de datos se regula en la LOPD y en el RLOPD que establecen como regulación supletoria lo establecido por la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (arts. 35.2 LOPD y 115 RLOPD). Esta aplicación supletoria de la regulación común es discutida por algún autor[1281].

Son aplicables los principios generales de la potestad sancionadora de la administración extraídos de los artículos 24 y 25 CE: legalidad, tipicidad, culpabilidad, presunción de inocencia, responsabilidad, *non bis in idem*, proporcionalidad y prescripción[1282]. Asimismo, también deben aplicarse las garantías constitucionales de los procesos como el derecho de defensa y el derecho de prueba[1283].

Los procedimientos pueden iniciarse de oficio o a instancia de algún afectado. De hecho, esta vía consistente en interponer una denuncia ante las autoridades es la más utilizada para combatir las vulneraciones del derecho, pese a no poder suponer ninguna

[1281] Sin embargo, VALERO TORRIJOS y FERNÁNDEZ SALMERÓN argumentan que en virtud del artículo 2.2 Ley 30/1992 y del artículo 2.1 Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos existe un conflicto con la supletoriedad establecida por el artículo 35.2 LOPD. Estiman estos autores que las normativas del procedimiento administrativo común deben prevalecer por encima de la regulación de la LOPD, con el fin de asegurar una aplicación homogénea en todas las Administraciones Públicas. J. VALERO TORRIJOS, M. FERNÁNDEZ SALMERÓN, "Procedimientos administrativos tramitados por la Agencia Española de Protección de Datos", R. MARTÍNEZ MARTÍNEZ (Coord.). *Protección de datos: comentarios a la LOPD y su reglamento de desarrollo, op. cit.*, págs. 267 a 269.

[1282] M. VIZCAÍNO CALDERÓN, *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, *op. cit.*, págs. 448 a 451. J. GUERRERO ZAPLANA, "Artículo 43. Responsables", C. LESMES SERRANO (Coord.), VVAA, *La Ley de protección de datos: análisis y comentario de su jurisprudencia*, *op. cit.*, págs. 625 a 629.

[1283] M. VIZCAÍNO CALDERÓN, *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, *op. cit.*, págs. 448 a 451.

compensación para el afectado por la vulneración[1284]. En los procedimientos seguidos ante las autoridades de control españolas el afectado denunciante mantiene una posición secundaria, ya que incluso sin su aquiescencia, se puede seguir de oficio el procedimiento[1285].

Hay que recordar que la resolución adoptada en el procedimiento sancionador agota la vía administrativa (art. 48.2 LOPD) y se puede acceder a la jurisdicción contencioso-administrativa.

Además de las sanciones económicas se contempla la potestad de inmovilizar los ficheros en caso de infracción grave o muy grave cuando se pudiera producir un grave menoscabo de los derechos fundamentales de los afectados (art. 49 LOPD).

[1284] ORDÓÑEZ SOLÍS realiza un paralelismo entre la *private enforcement* del derecho de la competencia europeo y del derecho a la protección de datos. En la aplicación del derecho de la competencia en la UE se distingue entre la aplicación pública o *public enforcement* y la aplicación privada o *private enforcement*. La aplicación pública supone la intervención de los organismos públicos de defensa de la competencia, como la Comisión Europea, y la aplicación privada supone la intervención de la empresa afectada por la cuestión de competencia que puede dirigirse a los tribunales. Pues bien, el autor indica que también se da esta dicotomía en el derecho a la protección de datos, de forma que en la aplicación pública participaría el Supervisor Europeo o las autoridades de control nacionales y la aplicación privada es la que ejercería el ciudadano afectado por la violación de su derecho a la protección de datos personales que podrá dirigirse a los tribunales, ya sea al TJUE si la acción se dirigiera contra las instituciones y organismos de la Unión o a los tribunales nacionales si se reclama contra particulares o contra autoridades nacionales. En España, la aplicación privada contra los particulares se canaliza a través de la jurisdicción civil y social y cuando es contra las Administraciones se canaliza a través de la jurisdicción contencioso-administrativa. Pues bien, este autor indica que la *private enforcement* pese a ser el procedimiento más genuino ha sido desplazada por la pujanza de los organismos de intervención propios del Estado de bienestar. D. ORDÓÑEZ SOLÍS, *Privacidad y protección judicial de los datos personales, op. cit.*, págs. 146 a 147, 202 a 207.

[1285] E. CALVO ROJAS, "El régimen sancionador de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. El principio de proporcionalidad", HUERGO LORA, A. (et al.). *La Potestad sancionadora de la Agencia Española de Protección de Datos*. Aranzadi, Agencia Española de Protección de Datos, Cizur Menor (Navarra), 2008, pág. 25. Este autor cita la SAN de 4 de abril de 2002 (Sala de lo contencioso-administrativo) (ROJ: SAN 2028/2002) (de la que además fue ponente en la Audiencia Nacional), en la que, si bien la retirada de la denuncia por parte del denunciante se afirma que no tiene relevancia al carecer el denunciante de poder de disposición sobre ella y sobre el curso del procedimiento sancionador, sí se tiene en cuenta al manifestar en el escrito de retirada no haber sufrido perjuicio económico derivado de la conducta denunciada y rebajar la infracción de grave a leve. El arrepentimiento del denunciante no pararía el procedimiento y en caso de que la autoridad considere que existe vulneración seguirá adelante hasta el final. Ejemplo de ello es la Resolución R/00347/2010 de la AEPD de 22 de febrero de 2010 en procedimiento nº PS/304/2009 (FJ IV), en el que pese a que el denunciante desiste de la denuncia no se tiene en cuenta, ya que como indica el procedimiento se inicia de oficio por el Director de la AEPD y es competencia de éste determinar si ha sido vulnerada la normativa de protección de datos. http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2010/common/pdfs/PS-00304-2009_Resolucion-de-fecha-22-02-2010_Art-ii-culo-4-y-4.3-LOPD.pdf (fecha consulta: 14.8.2014).

El marco sancionador establecido en la LOPD contiene uno de los regímenes más estrictos de la UE. Mientras en España se puede imponer una multa de hasta 600.000 euros, en otros países no se llega ni a los 10.000 euros o ni siquiera se sanciona, como en el Reino Unido donde no impusieron multas hasta el año 2010[1286]. Como consecuencia de la importancia de estas sanciones surgieron incluso pólizas de seguro que pretendían cubrir las pérdidas pecuniarias producidas por la imposición de estas sanciones[1287].

Siempre se ha criticado el elevado importe de las multas, que sólo se sancionara económicamente al sector privado y que no se tuvieran en cuenta factores como el tamaño de la empresa a la hora de imponer las sanciones. A raíz de estas demandas, se procedió a modificar esta regulación en el año 2011 con el fin de suavizar y flexibilizar estas sanciones[1288]. Es sorprendente que esta esperada reforma que llevaba tantos años debatiéndose se aprobara en trámite de enmiendas en el Senado, mediante una ley que nada tenía que ver con la materia y sin ser objeto de debate alguno[1289].

[1286] En algunos países las sanciones máximas no llegan a los 10.000 euros como por ejemplo sucede en Holanda, Chipre o en Croacia. Se señala en un estudio realizado por la FRA que en algunos países las autoridades de control no imponen sanciones, como en Bélgica, Dinamarca, Lituania, Hungría, Austria, Polonia y Suecia, aunque en estos casos sí que se establecen posibles multas en el ámbito penal que pueden imponer las autoridades judiciales. *Data protection in the European Union: the role of national data protection authorities, strengthening the fundamental rights architecture in the EU II, op. cit.*, pág.34. El volumen de sanciones económicas declaradas en el 2013 impuestas por la AEPD creció un 6,10 % respecto al año anterior, alcanzando la cifra de 22.339.440 euros, sin embargo en el 2014 decrecieron en un 23,89%, ya que ascendieron a 17.002.622 euros, Memoria de la AEPD de 2014, pág. 110.
Desde el 6 de abril de 2010 la *Information Commissioner's Office* (ICO), que es la autoridad de control de protección de datos del Reino Unido, puede imponer sanciones en caso de incumplimiento de la Ley inglesa que pueden llegar a 500.000 libras, lo que equivale casi a los 600.000 euros de la sanción más grave en la ley española. Las Secciones 55A a 55E de la Ley inglesa se modificaron para incluir la posibilidad de que el ICO pudiera sancionar con multas a los responsables. *Data Protection Act 1998 Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998, ICO, The Stationery Office, 2012, London.* http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ico_guidance_on_monetary_penalties.pdf (fecha consulta: 14.8.2014).

[1287] La Dirección General de Seguros y Fondos de Pensiones en su Boletín Diario de Seguros del 2 de junio de 2008, en respuesta a una consulta sobre si era posible asegurar multas penales, indicó que era contrario al orden público. Esta respuesta no es vinculante. Claramente en contra de esta postura y en defensa de este tipo de pólizas: J.M. ELGUERO, "El seguro de responsabilidad civil por protección de datos personales", *Revista de responsabilidad civil y seguro*, págs. 47 a 80 http://www.asociacionabogadosrcs.org/doctrina/doctrina02.pdf?phpMyAdmin=9eb1fd7fe71cf931d588191bc9123527 (fecha consulta: 16.7.2015).

[1288] La modificación se introdujo en la Ley 2/2011, de 4 de marzo, de Economía Sostenible (BOE núm. 55 5.3.2011), Disposición final quincuagésima sexta. Esta ley también fue conocida por introducir la llamada Ley Sinde en materia de derechos de propiedad intelectual.

[1289] J.L. PIÑAR MAÑAS, *Protección de datos: importante reforma del régimen sancionador*, http://www.abogados.es (fecha consulta: 30.3.2011).

Uno de los aspectos que se cambiaron fueron los tramos de las sanciones (art. 45, apartados 1 a 3). Si bien el tramo más elevado de las sanciones muy graves se mantuvo igual (multa de 300.001 a 600.000 euros), se modificaron los otros. Las infracciones leves pasaron de ser sancionadas con multa de 600 a 60.000 euros a ser sancionadas con multa de 900 a 40.000 euros y las graves pasaron de ser sancionadas con multa de 60.000 a 300.000 euros a multa de 40.001 a 300.000 euros[1290]. Por tanto, se intentó que los tramos de leves y graves pudieran optar a un importe menor.

También se hicieron cambios en el catálogo de las tipificaciones de las infracciones. Hay que resaltar, por ejemplo, en las infracciones leves, a las que se incorporó la transmisión de datos a un encargado del tratamiento sin cumplir con la exigencia de tener un contrato de acuerdo con lo establecido en el artículo 12 LOPD. En la regulación anterior, el hecho de no tener este contrato se podía considerar como infracción muy grave al entender que se trataba entonces de una cesión ilícita, ya que no contaba con un tipo tan específico (actual art. 44.2.d LOPD)[1291].

Respecto a las infracciones graves, se incluyó la relativa a la vulneración del deber de secreto que antes era leve (art. 44.3.d LOPD). Se amplió la infracción referida a recabar datos sin consentimiento del titular de los datos que ahora es grave, mientras que en la regulación anterior sólo era infracción grave si el consentimiento debía ser expreso porque lo requería la ley (art. 44.3.b LOPD). La comunicación de datos sin tener legitimación para ello descendió de la categoría de muy grave a grave (art. 44.3.k LOPD). Se limitó la infracción relativa al tratamiento de datos con conculcación de los principios y garantías establecidos en la ley, tipo genérico, que en la actual redacción se ha

[1290] Hay que decir que además de redondear los importes se corrigió un defecto en los tramos, ya que el límite máximo de la sanción coincidía con el importe mínimo del siguiente tramo. J. GÓMEZ NAVAJAS, "Tipos de sanciones en la Ley Orgánica 15/1999, de protección de datos", A. TRONCOSO REIGADA, (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, págs. 2.140 a 2.141.

[1291] A esta infracción se le suman otros supuestos en la categoría de infracciones leves. Los supuestos que se mantienen sin cambios son: no remitir a la AEPD las notificaciones previstas en la ley; no solicitar la inscripción del fichero en el Registro General de Protección de Datos (art. 44.2.a y b LOPD). Otro supuesto sufre sólo un pequeño cambio: incumplir el deber de informar cuando los datos se recabaran directamente del interesado (art. 44.2.c LOPD). En este caso en la regulación anterior no se especificaba que el supuesto se refiriera únicamente al caso de recogida directa. Se elimina del catálogo de infracciones leves el supuesto de no atender la solicitud de rectificación o cancelación por motivos formales que se hallaba en el anterior artículo 44.2.a LOPD. Asimismo el anterior artículo 44.2.e LOPD que contemplaba el incumplimiento del deber de secreto se elimina, al incorporarse al catálogo de infracciones graves.

transformado en específico, ya que se refiere a los principios y garantías establecidos en el artículo 4 LOPD relativo al principio de calidad (art. 44.3.c LOPD)[1292].

También en las infracciones graves se modificó la relativa al ejercicio de derechos, que antes se contenía en dos supuestos y actualmente se incluye sólo en uno (art. 44.3.e LOPD)[1293]. Se mantiene la infracción por incumplimiento del deber de información cuando los datos no hayan sido recabados del interesado (art. 44.3.f LOPD)[1294]. Por último, se añadió la infracción sobre el incumplimiento de los restantes deberes de notificación o requerimiento al afectado impuestos por la ley o las disposiciones de desarrollo, de forma que se pudiera cerrar cualquier posible incumplimiento relacionado con este aspecto (art. 44.3.g LOPD)[1295].

En las infracciones muy graves se redujeron los supuestos tipificados. Uno de los tipos eliminados fue el referente al tratamiento de datos de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales, otro tipo genérico[1296].

[1292] Este tipo genérico había sido considerado como un tipo autónomo y general. Se consideraba que recogía la infracción típica del régimen de protección de datos y se había planteado su constitucionalidad por dudar si cumplía con el principio de legalidad. A.E. DE ASÍS ROIG, F. J. GÓNZALEZ ESPADA, "Tipos de infracciones", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.,* págs. 2.048 a 2.051.

[1293] Los supuestos del anterior artículo 44.3, apartados d y e LOPD, se han incorporado en la infracción relativa al impedimento u obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

[1294] Aunque se elimina la alusión que el anterior artículo 44.3.l LOPD realizaba a los artículos 5, 28 y 29 LOPD.

[1295] Además se mantuvieron sin apenas sufrir ningún cambio los siguientes supuestos incluidos en el actual artículo 44.3 apartados a, h, i, j: proceder a crear ficheros de titularidad pública o iniciar la recogida de datos para estos ficheros sin autorización de disposición general, publicada en el boletín pertinente; mantener los ficheros, locales, programas o equipos que contengan datos sin las debidas condiciones de seguridad; no atender los requerimientos o apercibimientos de la AEPD o no proporcionarle los documentos e informaciones solicitados; obstruir la actividad inspectora. Se eliminaron de esta categoría los siguientes supuestos del anterior artículo 44.3, apartados b y k: proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad; no inscribir el fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando haya sido requerido para ello por el Director de la AEPD.

[1296] Además del mencionado se eliminaron los siguientes tipos que se hallaban en el anterior artículo 44.4 LOPD (apartados f a i): la vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas; no atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición; no atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Quedaron como infracciones muy graves apenas sin cambios: la recogida de datos en forma engañosa o fraudulenta; tratar o ceder los datos especialmente protegidos salvo en los casos en los que se prevea[1297]; no cesar en el tratamiento ilícito de datos cuando se hubiera requerido por la AEPD y la transferencia internacional de datos con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la AEPD, salvo si ello está permitido por la ley (art. 44.4, apartados a a d LOPD).

Una cuestión muy importante y que respondía a una de las reivindicaciones indicadas era la relativa a la gradación de las sanciones. Ya se incorporaban criterios para reducir las sanciones, en el anterior marco sancionador (art. 45.4 LOPD)[1298], así como la posibilidad de que, ante una cualificada disminución de la culpabilidad del imputado o de la antijuricidad del hecho, se pudiera aplicar la escala inferior de sanciones.

Es habitual que la infracción se produzca por un error y que se alegue, por tanto, la falta de culpabilidad[1299]. Sin embargo, se reitera en estos casos que la imputación puede realizarse a título de mera inobservancia, por incumplimiento del deber de diligencia[1300]. Esta simple inobservancia, según la jurisprudencia, no puede entenderse como la admisión de la responsabilidad objetiva, sino que se requiere la existencia de dolo o culpa[1301].

[1297] En este supuesto se añadió la cesión además del tratamiento en el supuesto.

[1298] La cuantía de las sanciones se valoraba atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

[1299] Es un argumento recurrente utilizado por los responsables el de alegar que la vulneración del derecho fue ocasionada por un error involuntario con ausencia total de intencionalidad. Citar como ejemplo SAN de 22 de junio de 2006 (Sala de lo contencioso-administrativo) (ROJ: SAN 3072/2006), FJ 6.

[1300] Así lo establece el artículo 130 Ley 30/1992. En este sentido, el Tribunal Supremo manifestó que "dada la especial sensibilidad de los bienes en juego dentro del campo del tratamiento de datos, las entidades que se benefician de dicho tratamiento tienen que ser especialmente diligentes en el cumplimiento de las garantías legales, sin que sea factible escudarse en errores de configuración de los programas que la entidad debió prever con el empleo de una mayor diligencia" STS de 23 de enero de 2007 (Sala 3ª) (ROJ: STS 224/2007), FJ 2. A.E. DE ASÍS ROIG, F. J. GÓNZALEZ ESPADA, "Tipos de infracciones", A. TRONCOSO REIGADA (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, pág. 2.069.

[1301] SSTS 12 de diciembre de 1995 (Sala 3ª) (ROJ: STS 6316/1995) FJ 3 y de 18 de marzo de 2005 (Sala 3ª) (ROJ: STS 1730/2005) FJ 4, SAN de 25 de mayo de 2006 (Sala de lo contencioso-administrativo) (ROJ: SAN 2284/2006), FJ 5 y STC 76/1990 de 26 de abril de 1990.

Lo cierto es que, por regla general, cuando se estima que el responsable cometió un error, se concluye habitualmente que existió culpabilidad, al argumentar que debió haber desplegado la diligencia debida. Ello, sin perjuicio de alguna sentencia excepcional que haya considerado que la infracción, por mera negligencia, no puede conducir a que todo error por nimio que sea ha de ser considerado como infracción de la legislación de protección de datos[1302].

Como contrapeso, se puede señalar que habitualmente se aplica también el principio de proporcionalidad, de forma que se gradúa la sanción en función de la gravedad de la conducta[1303].

Con la reforma se incluyeron hasta diez criterios para graduar las sanciones y cinco para descender en la escala aplicable. Respecto a los criterios para graduar las sanciones se añadieron los siguientes: el carácter continuado de la infracción, la vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal, el volumen de negocio o actividad del infractor; la acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor (art. 45.4, apartados a, c, d, i LOPD).

[1302] SAN de 17 de marzo de 2004 (Sala de lo contencioso-administrativo) (ROJ: SAN 1914/2004) citada por E. CALVO ROJAS, "El régimen sancionador de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. El principio de proporcionalidad", HUERGO LORA, A. (et al.). *La Potestad sancionadora de la Agencia Española de Protección de Datos*, *op. cit.*, pág. 25. En esta sentencia se considera que la entidad bancaria sancionada por la AEPD cometió un error nimio y se anula la resolución de la AEPD. El banco anotó una operación en una cuenta bancaria que no había sido ordenada por los titulares de la cuenta. La Audiencia indica que se trata de una anomalía en la mecánica bancaria por la que se incoó un expediente ante la Comisión Nacional del Mercado de Valores que fue archivado sin declaración de responsabilidad. Así se establece que debe tenerse en cuenta el carácter restrictivo que debe presidir la actuación administrativa sancionadora y estimar desproporcionado que cualquier error de anotación pueda implicar una infracción (además grave en este caso) de la LOPD. FJ 4.

[1303] "Artículo 131. Principio de proporcionalidad. 1. Las sanciones administrativas, sean o no de naturaleza pecuniaria, en ningún caso podrán implicar, directa o subsidiariamente, privación de libertad. 2. El establecimiento de sanciones pecuniarias deberá prever que la comisión de las infracciones tipificadas no resulte más beneficioso para el infractor que el cumplimiento de las normas infringidas. 3. En la determinación normativa del régimen sancionador, así como en la imposición de sanciones por las Administraciones Públicas se deberá guardar la debida adecuación entre la gravedad del hecho constitutivo de la infracción y la sanción aplicada, considerándose especialmente los siguientes criterios para la graduación de la sanción a aplicar: a) La existencia de intencionalidad o reiteración. b) La naturaleza de los perjuicios causados. c) La reincidencia, por comisión en el término de un año de más de una infracción de la misma naturaleza cuando así haya sido declarado por resolución firme." Ley 30/1992.

Con estos criterios se respondió a la demanda que había de adaptación de la sanción al sujeto obligado. Este aspecto ha sido muy polémico, ya que se argüía en defensa de su no incorporación que estamos ante un derecho fundamental y, por tanto, no debía modularse la sanción en función de la tipología del sujeto obligado, sino que debía ser neutra y debería sancionarse en función únicamente de si se encaja la infracción en alguno de los tipos. No obstante, lo cierto es que no tiene la misma repercusión punitiva una sanción, por ejemplo, de 300.000 euros para una gran multinacional, que para una micropyme o un autónomo.

Por ello, se tendrá en cuenta el volumen de negocio de la organización y también la actividad del infractor, de forma que si esta actividad está ligada fuertemente a la realización de tratamientos de datos, sin duda se le debería demandar una diligencia más elevada que a un infractor que sólo trate datos de forma accesoria a su actividad. Asimismo también se tendrá en cuenta la implantación de los procedimientos adecuados de actuación en la recogida y tratamiento de datos. De esta forma, se tiene en cuenta la adopción de estos procedimientos, aunque no funcionen. Por otro lado, esto significa también que, pese a que se implanten estos procedimientos si fallan, se sancionará, aunque pueda reducirse esa sanción.

Los criterios para descender de escala en las sanciones no existían en la regulación anterior, por lo que es positivo que se haya clarificado cuando puede producirse. Estos criterios son los siguientes: cuando se puedan aplicar varios criterios de graduación; cuando la entidad infractora haya regularizado la situación irregular de forma diligente; cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción; cuando el infractor haya reconocido espontáneamente su culpabilidad; cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente (art. 45.5 LOPD).

Otra novedad muy importante que ayudó a suavizar el marco sancionador fue la introducción de la figura del apercibimiento. El apercibimiento permite que, de forma excepcional, en virtud de la naturaleza de los hechos y de la concurrencia de los criterios indicados para descender de escala en el catálogo, se pueda no acordar la apertura del procedimiento sancionador e instar, en cambio, al sujeto infractor para que adopte las

medidas correctoras. Eso sí, sólo para infracciones leves o graves y si no se hubiera sancionado o apercibido nunca. Si no se atendiera el apercibimiento se podría abrir un procedimiento sancionador. No obstante su carácter excepcional, lo cierto es que, desde la modificación del marco sancionador, la AEPD ha utilizado profusamente esta figura[1304].

Tanto de la aplicación de los criterios de graduación de las sanciones, como de la utilización de la figura del apercibimiento se deriva la necesidad de atenuar un régimen demasiado estricto y, por tanto, generador de opiniones negativas, especialmente entre aquellas empresas de reducido tamaño aglutinadoras de un elevado número de obligaciones que ponen a prueba su diligencia y los recursos que puedan invertir en un contexto económico de gran dificultad[1305].

La actuación de las autoridades de control quedaría sometida al control judicial de los tribunales contencioso-administrativos[1306]. Las resoluciones de las autoridades se verán sometidas al control jurisdiccional que, respecto a los procedimientos sancionadores, podrán promover las partes afectadas por la resolución sancionadora[1307]. De esta forma, si el responsable no estuviera de acuerdo con la decisión de la autoridad la podrá recurrir.

[1304] En el año 2014 la AEPD estableció 260 infracciones en materia de protección de datos en las que impuso sanciones sin atenuación, 194 infracciones a las que aplicó el apercibimiento y 442 sanciones a las que aplicó una sanción de la escala precedente de gravedad. Memoria de 2014 AEPD, pág. 105.

[1305] Así, en la comparecencia que realizó el Director de la AEPD, don José Luis Rodríguez Álvarez, al presentar la Memoria de la AEPD del año 2011, se felicitó de la reforma realizada que permitía adaptarse al tipo de responsable y de la amplia utilización de la figura del apercibimiento: "A la luz de la experiencia acumulada en estos meses de aplicación, se puede afirmar que la reforma se ha mostrado adecuada para alcanzar los objetivos perseguidos, dado que ha permitido modular y atenuar las sanciones en función de las circunstancias concurrentes en cada caso y diferenciar convenientemente en atención a la diligencia y a la responsabilidad exigible según se trate de grandes empresas, de pequeñas y medianas empresas o que los infractores hayan sido profesionales o personas físicas. Especialmente indicada se ha mostrado la figura del apercibimiento, que permite amonestar sin imponer sanciones económicas a determinados responsables en el caso de que se trate de la primera infracción. La agencia está haciendo un uso frecuente de esta posibilidad, como queda de manifiesto en el hecho de que de las 706 resoluciones de infracción relativas a responsables privados dictadas desde la entrada en vigor de la reforma en marzo de este año, 312 han sido de apercibimiento, lo que supone un 44 % del total, siendo aún mayor su repercusión en el ámbito de la videovigilancia, donde el 70 % de las infracciones declaradas se han saldado con un apercibimiento, sin sanción económica." Intervención del Director de la AEPD don José Luis Rodríguez Álvarez. Cortes Generales, Diario de Sesiones del Congreso de los Diputados, Comisiones Constitucional, X Legislatura, núm. 205, sesión del 7 de noviembre de 2012, pág. 3.

[1306] La Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contencioso-administrativa en su disposición adicional cuarta, apartado 5, establece que los actos y disposiciones dictados por la AEPD serán recurribles directamente ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional.

[1307] STS de 25 de marzo de 2014 (Sala 3ª) (ROJ:STS 1203/2014), FJ 2.

Respecto a este control judicial, cabe destacar una sentencia del Tribunal Supremo de 2 de diciembre de 2011 que resolvió un recurso de casación y consideró que la AEPD no podía supervisar a los órganos judiciales[1308]. El Alto tribunal estimó que la independencia del poder judicial impedía cualquier tipo de injerencia por parte de una autoridad administrativa, como es la AEPD, por lo que atribuyó esta competencia al Consejo General del Poder Judicial[1309].

No obstante, también cabe apuntar la utilidad que, a veces, tiene para el afectado la iniciación de un procedimiento ante las autoridades de control. Y es que tras las acciones derivadas de la actuación de la autoridad de control, el afectado puede continuar con una demanda de indemnización presentada ante un tribunal, así como también puede presentar la misma sin necesidad de que exista el procedimiento ante la agencia[1310].

c. La impunidad del sector público

Si ha habido una cuestión polémica en lo que se refiere al marco sancionador de la LOPD, además de los elevados importes de las multas, ha sido la diferencia entre las consecuencias que un incumplimiento de lo establecido en esta legislación tiene

[1308] STS de 2 de diciembre de 2011 (Sala 3ª) (ROJ: STS 8497/2011).

[1309] El Director de la AEPD informaba del contenido de esta sentencia en su comparecencia ante el Congreso de Diputados para presentar la Memoria de 2011 y comunicaba el inicio de un diálogo con el Consejo General del Poder Judicial para determinar los efectos de la sentencia y trasladar los expedientes ya iniciados. No obstante, indicaba el Director la dificultad de dar aplicación a la sentencia la mezclarse en el ámbito de la Administración de Justicia ficheros de distinta naturaleza que tenían responsables que podían ser órganos judiciales u órganos administrativos. Por ello, sugería el Director la intervención del legislador para aclarar las competencias de la AEPD. Cortes Generales, Diario de Sesiones del Congreso de los Diputados, Comisiones Constitucional, X Legislatura, núm. 205, sesión del 7 de noviembre de 2012, págs. 3 a 4.

[1310] En todo caso esto plantea la necesaria coherencia entre las decisiones que se adopten, tanto por las autoridades de control, como por los tribunales en los casos de indemnización. Al igual que sucede en el derecho europeo de la competencia se podría distinguir en materia de protección de datos entre las acciones *follow-on* o *stand alone*. Las acciones *follow-on* son las que interponen los particulares aprovechando decisiones previas de las autoridades de competencia. En cambio las acciones *stand alone* son las reclamaciones independientes que ejercitan los particulares sin fundarse en decisiones administrativas previas. ORDÓÑEZ SOLÍS remite a lo apuntado por el Tribunal Constitucional en STC 160/2008, de 2 de diciembre, (FJ 7) en la que indicó que unos mismos hechos no pueden existir y dejar de existir para los órganos del Estado según la perspectiva jurídica que se adopte. De esta forma, según este autor pese a las diferentes vías posibles para la aplicación pública y la aplicación privada del derecho a la protección de datos, debería asegurarse una coherencia entre las decisiones que se adopten en virtud de las mismas. D. ORDÓÑEZ SOLÍS, *Privacidad y protección judicial de los datos personales*, *op. cit.*, págs. 215 a 216. La postura de este autor contrasta con la valoración diversa que hemos visto debe realizarse desde los órdenes civil y administrativo.

dependiendo de si el infractor es del sector privado o del sector público[1311]. En el primer caso, la infracción conllevará una sanción que puede consistir en una multa. En el segundo caso, la consecuencia será la notificación por parte de la AEPD de las medidas correctoras que deberá adoptar el sujeto infractor, así como la posible propuesta de iniciación de actuaciones disciplinarias.

Si bien la argumentación de esta no imposición de multas es la caja única de las administraciones[1312], lo cierto es que podría conectarse esta carencia de sanciones con el escaso incumplimiento de la normativa por parte de este sector[1313]. Al lado de esta carencia de sanción, se establece, como ya se ha visto, la posibilidad de los afectados de demandar a las administraciones públicas por daños (art. 19 LOPD). Es decir, se iguala a ambos sectores respecto a la responsabilidad civil pero no en el ámbito administrativo.

También la modificación del marco sancionador de la LOPD afectó a esta regulación relativa a las infracciones administrativas de las Administraciones Públicas. De esta forma, si en la anterior regulación se centraban las infracciones cometidas en ficheros de los que fueran responsables las administraciones públicas, en la redacción actual esto se matiza, de forma que se especifica que las infracciones serán "cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza" (art. 46.1 LOPD).

[1311] Recoge estas críticas M. VIZCAÍNO CALDERÓN, *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, págs. 506 a 509.

[1312] En la misma comparecencia referida en la anterior nota, de noviembre de 2012, el Director de la AEPD hizo alusión a esta dualidad que en el actual proyecto de reforma de la Unión Europea, como se verá más adelante no existe: "En el proyecto se prevé un régimen de sanciones económicas sin distinguir entre el sector público y el sector privado y obviamente esto es un cambio significativo que deberá ser valorado. Hay buenas razones para mantener el sistema que tenemos en España. Básicamente siempre se ha entendido que, al tratarse de un presupuesto público, en definitiva podría entenderse que es una caja única y tiene poco sentido imponer sanciones a administraciones públicas para que vayan a la caja de la Administración General del Estado o de la Administración pública en general, y sobre todo siempre se ha entendido que, si se impone una sanción económica a una Administración —pensemos por ejemplo en un ayuntamiento—, puede existir un riesgo de que esa sanción afecte al normal funcionamiento de los servicios y que en última instancia quienes realmente se vean afectados por la sanción impuesta a la Administración pública sean los ciudadanos. Estas son las razones por las que en España hasta ahora hemos optado por no imponer sanciones económicas a la Administración pública cuando se producen infracciones del régimen de protección de datos, pero también es cierto que desde el sector privado esto se considera un agravio comparativo y continuamente tenemos quejas, en parte fundadas, que cuestionan este distinto trato." *Ibídem*, pág. 16.

[1313] Se puede ilustrar este escaso cumplimiento con el número acumulado de ficheros inscritos en 2014 que en el caso de ficheros de titularidad privada ascendía a 3.594.106 y en el caso de ficheros de titularidad pública a 152.824. Memoria de 2014 de la AEPD, pág. 131.

Este cambio es muy ambiguo y parece responder a varios objetivos. Uno sería la necesidad de cubrir no sólo los ficheros sino también los tratamientos. Otro objetivo, que parece más probable sería dejar claro que, pese a que no se haya considerado que estemos ante un fichero de titularidad pública, si efectivamente se está ante uno, también se podrá actuar, aunque, por ejemplo, no se hubiese publicado la disposición general pertinente.

Además también se modificó la remisión que, en caso de ficheros de titularidad pública, se hacía respecto a las sanciones y procedimiento a aplicar. Y es que la remisión que se hacía era a un precepto que establece que el procedimiento y las sanciones a aplicar son las establecidas en la legislación sobre el régimen disciplinario de las Administraciones Públicas (art. 43.2 que remitía al 46.2 LOPD). Lo que se hizo fue corregir esta remisión para que ahora remita a los preceptos dedicados a las infracciones de las Administraciones (art. 46 LOPD) y al procedimiento sancionador (art. 48 LOPD). No obstante, dadas las especiales características de estos procedimientos se diferencian mediante la denominación de procedimientos de declaración de infracción de administraciones públicas.

2.6. Las exclusiones de responsabilidad en la normativa sobre comercio electrónico

La Directiva sobre comercio electrónico contiene unas disposiciones específicas sobre la responsabilidad de los prestadores de servicios de intermediación de la sociedad de la información[1314]. Debido a la importancia de estos servicios para el funcionamiento de Internet, se les adjudicó un estatuto especial en materia de responsabilidad. De esta forma no serán responsables por los contenidos ilícitos a los que puedan acceder en el desarrollo de sus servicios si se cumplen una serie de requisitos que varían según el tipo de servicio. Los requisitos apuntan a la naturaleza de los servicios que es básicamente tecnológica, de forma que, mientras se mantenga la neutralidad en el desarrollo del servicio, no se les podría atribuir responsabilidad.

En la regulación de la directiva los servicios que se consideran dentro de esta categoría de intermediación son tres: los de mera transmisión, los de memoria tampón o *caching* y los de alojamiento de datos. Este régimen se completa con la obligación

[1314] Artículos 12 siguientes de la Directiva 2000/31/CE.

dirigida a los Estados miembros de no imponer a estos intermediarios una obligación general de supervisar los datos que transmitan o almacenen ni de realizar búsquedas activas de contenidos ilícitos (art. 15 Directiva 2000/31/CE)[1315].

En el ordenamiento jurídico español este régimen se ha trasladado a los artículos 13 ss. LSSI. No obstante, a diferencia de la Directiva 2000/31/CE, la LSSI ha añadido otro servicio de intermediación: el de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda (art. 17 LSSI)[1316].

Este régimen de exclusión de responsabilidad se ha estimado que es de carácter transversal, de forma que excluiría cualquier tipo de responsabilidad (penal, civil o administrativa)[1317]. Por tanto, serviría para excluir la responsabilidad que se pudiera derivar de un contenido ilícito que vulnerara la normativa de protección de datos.

Esta regulación ha abierto multitud de debates sobre diversas cuestiones que, además se han suscitado en la jurisprudencia reciente. Entre los aspectos debatidos figura el del papel que debe atribuirse a estos servicios: el de asumir un papel neutral o, por el contrario, de imponerles un papel de vigilantes de los contenidos que pasan por sus manos[1318]. En este sentido, se ha producido una pugna entre la postura de la AEPD y el buscador *Google* que ha dado como resultado una sentencia del TJUE sobre el derecho al olvido[1319]. Esta sentencia se abordará en el siguiente capítulo con más detalle, donde se

[1315] Respecto a esta obligación citar las sentencias del TJUE de 24 de noviembre de 2011, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, EU:C:2011:771 y de 16 de febrero de 2012, *SABAM/Netlog NV*, C-360/10, EU:C:2012:85, que estimaron que obligar a prestadores de servicios de Internet a instalar un sistema de filtrado para detectar vulneraciones de los derechos de autor era contrario al derecho europeo.

[1316] En la Directiva 2000/31/CE se hacía referencia a que la Comisión presentaría un informe sobre la aplicación de la directiva en el que analizaría la necesidad de presentar propuestas sobre la responsabilidad de proveedores de hipervínculos y servicios de instrumentos de localización. En el primer informe señalaba PEGUERA POCH que no realizó ninguna propuesta concreta sobre esta cuestión sino que manifestó que en algunos Estados miembros se habían establecido las exclusiones para estos servicios. M. PEGUERA POCH, *La exclusión de responsabilidad de los intermediarios en Internet*, Comares, Granada, 2007, pág. 228.

[1317] Esta es una de las diferencias que apuntaba PEGUERA POCH de este sistema respecto a las limitaciones de responsabilidad de la *Digital Millenium Copyright Act*, norma de EEUU inspiradora del mismo. En la norma estadounidense el enfoque es vertical, de forma que sólo se excluye la responsabilidad en materia de *copyright* y respecto a la responsabilidad civil. *Ibídem*, págs. 218 a 226.

[1318] A este respecto ver el interesante trabajo sobre la necesidad de reformular el concepto constitucional de censura en la era digital: M.J. GARCÍA MORALES, "La prohibición de la censura en la era digital", *Teoría y realidad constitucional*, núm. 31, 2013, págs. 237 a 276.

[1319] Sentencia del TJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2014:317.

retomará el debate sobre el papel de los buscadores ante las solicitudes de cancelación de enlaces a contenidos que están publicados lícitamente en sitios web.

PARTE III
LAS NUEVAS TECNOLOGÍAS Y EL RESPONSABLE: RETOS Y RESPUESTAS

Una vez analizado el papel de la figura del responsable en el pasado y el presente del panorama normativo, procede examinar cómo esta figura se enfrenta a nuevos retos. La situación actual es enormemente compleja para el derecho a la protección de datos y obliga a reflexionar sobre la validez y la eficacia del concepto de responsable.

Realmente, ¿esta figura responde a los nuevos retos planteados? Pero, ¿de qué retos exactamente hablamos? ¿Qué se está haciendo para dar esa respuesta? ¿Qué hacen los gobiernos, los legisladores, los tribunales, los responsables y los ciudadanos? Mediante esta parte quiero también sumarme a esta respuesta global y arrojar algo de luz para vislumbrar si la figura del responsable mantiene vigencia y cual es su papel en este contexto evolutivo.

CAPÍTULO VIII
LA FIGURA DEL RESPONSABLE ANTE EL IMPACTO DEL DESARROLLO TECNOLÓGICO

1. RETOS Y TENSIONES PLANTEADOS POR EL CAMBIO EN EL CONTEXTO TECNOLÓGICO

¿Cuáles son los retos a los que se enfrenta la figura del responsable? Estos retos se articulan en una serie de tensiones a las que se somete al derecho a la protección de datos, fruto de los cambios en el contexto actual de nuestro mundo global. En este apartado se pretende responder a la pregunta ¿cómo hemos llegado hasta el momento actual? Para ello, se retoma el contexto que empezó a dibujarse en el inicio de este trabajo, para entender la complejidad del mismo y las tensiones originadas, especialmente, por enmarcarse en un entorno, como el digital.

1.1. La especial naturaleza de Internet y el poder público como un gran hermano digital

Las especiales características de Internet, instrumento protagonista en la revolución tecnológica, y las oscilaciones del péndulo histórico que nos llevan a un tira y afloja entre los valores de seguridad y protección de los derechos de los ciudadanos, componen el contexto actual.

1.1.1. Internet: un entorno global, sin territorio y ¿sin gobierno?

La evolución tecnológica viene marcada por el origen de Internet, en los años sesenta, que respondió a la creación, promovida por el Departamento de Defensa de los Estados Unidos, de un sistema de comunicaciones descentralizado. Tras su origen militar, el sistema se utilizó principalmente para la investigación científica y en 1995 se abrió al uso privado. La gestión de Internet, inicialmente en manos de organismos técnicos, pasó a las de organismos de carácter multisectorial, de forma que se preservó del control puramente gubernamental[1320]. Sin embargo, existen tensiones y los Estados, progresivamente, demandan un papel más relevante en el gobierno de Internet, que se ha convertido, además, en una pieza estratégica en materia de seguridad. Hay tantos intereses contrapuestos que se ha vuelto una cuestión difícil de resolver.

[1320] En la historia sobre el gobierno de Internet se pueden distinguir tres fases. En la primera fueron los organismos técnicos que habían creado Internet los que decidían acerca de su gestión. En la segunda etapa, que coincidiría con el éxito comercial de Internet, el gobierno se ejercería por organizaciones, como la *Internet Corporation for Assigned Names and Numbers* (ICANN) o el *Internet Governance Forum,* en las que se adoptó un enfoque multi-sectorial, de manera que los conformaban actores representantivos de todos los ámbitos afectados. Desde el año 2012 con la reunión de la Unión Internacional de Telecomunicaciones (UIT), en Dubai, se aprecia la presión de los Estados por tener un papel en el gobierno y regulación de Internet. S.J. SHACKELFORD, E. OTI, J.A. KERR, E. KORZAK, A. KUEHN, "Spotlight on cyber V: back to the future of Internet governance", *Georgetown Journal of International Affairs*, June 25, 2015, http://journal.georgetown.edu/back-to-the-future-of-internet-governance/ (fecha consulta: 20.5.2015). Respecto a la reunión mencionada de la UIT, hay que indicar que, se trata de un organismo de la Organización de Naciones Unidas, en el que los gobiernos se reúnen para desarrollar acuerdos sobre las telecomunicaciones. En esta reunión se revisaba el Reglamento Internacional de las Telecomunicaciones, que finalmente fue aprobado en diciembre de 2012, http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12-es.pdf (fecha consulta: 18.6.2014). Los medios de comunicación se hicieron eco de que, en las reuniones a puerta cerrada, que tenían lugar para revisar esta normativa, se estaba negociando, por parte de algunos países de régimen autoritario, la prohibición del anonimato en Internet o la posibilidad de filtrados e incluso de censura de contenidos. Finalmente, no se incluyeron estas medidas en el texto. Algunas voces críticas fueron las de Vinton Cerf, uno de los conocidos como "padres de Internet" y que era el evangelista de Internet de *Google*, V. CERF, "La lucha a favor de la libertad en Internet", *El País, Opinión*, 3.12.2012 http://elpais.com/elpais/2012/11/29/opinion/1354207036_281116.html, (fecha consulta: 18.12.2012) y T. GARTON ASH, "La Red como campo de batalla", *El País, Opinión*, 11.12.2012 http:/elpais.com/elpais/2012/12/07/opinion/1354876187_848856.html (fecha consulta: 18.12.2012).

Al originarse en los Estados Unidos, Internet nació, al amparo de los valores de la sociedad estadounidense, especialmente el de la libertad de expresión. Así, cabe recordar la declaración de inconstitucionalidad de la *Communications Decency Act* y la sentencia del Tribunal Supremo estadounidense que manifestó que debía protegerse el derecho de cualquier usuario de Internet de emitir información[1321].

No hay duda que Internet ha constituido una importante fuente de información y una herramienta potente de comunicación. De esta forma, se ha utilizado por los ciudadanos para luchar contra gobiernos, como ha sucedido en la revolución egipcia.

Ello ha hecho surgir la sombra de la represión, por parte de algunos gobiernos, en un afán de evitar este uso por parte de sus ciudadanos. Algunos países, como Turquía o China, han bloqueado el acceso a Internet desde su territorio[1322]. Ante estos peligros de interferencia del Estado en Internet, se ha proclamado la necesidad de preservar este espacio de libertad y se ha equiparado el derecho a la libertad de expresión, con el derecho de acceso a Internet[1323]. Para ello, se ha manifestado que los ciudadanos deben mantener intactos sus derechos en el entorno *online*[1324].

[1321] Ver Capítulo I.

[1322] Ejemplo de ello es la sentencia del TEDH de 18 de diciembre de 2012 *Yildirim c. Turquía*, en la que se condenó al gobierno turco por bloquear el acceso a *Google Sites*. El acceso se bloqueó fruto de la adopción de una medida cautelar, en un procedimiento judicial pero se realizó de forma general, por lo que además de bloquear el sitio web objeto de litigio se bloquearon otros no relacionados. El ciudadano reclamante era uno de los titulares de esos otros sitios web alojados en *Google Sites*, que vió impedido el acceso a su web. El TEDH consideró que se produjo una injerencia en el derecho a la libertad de expresión de este ciudadano turco, previsto en el artículo 10 CEDH. Esta injerencia no cumplía el primer requisito de venir regulada por ley, por lo que el TEDH ya no analizó los demás requisitos para poder establecer medidas restrictivas de derechos.

[1323] En este sentido, citar la sentencia de 10 de junio de 2009 del Consejo Constitucional francés (decisión núm. 2009-580 DC), que mencionaba el TEDH en el asunto *Yildirim c. Turquía.* En la misma se afirmó que, en la actualidad, debe entenderse que la libertad de expresión incluye el derecho de acceder a Internet y que la restricción del derecho al libre acceso público a los servicios de comunicación al público *on line* solo puede ser decretada por un juez, tras un proceso equitativo y debe ser proporcionada. Sentencia del TEDH de 18 de diciembre de 2012 *Yildirim c. Turquía*, apdo. 32.

[1324] Ejemplo de estas declaraciones es la Recomendación CM/Rec(2014)6 del Comité de Ministros del Consejo de Europa de 16 de abril de 2014, a la que se anexa una guía sobre los derechos humanos de los usuarios de Internet. Esta recomendación se dirige a los 47 Estados miembros del Consejo de Europa, con el fin de alertar sobre la importancia del respeto de los derechos humanos también en el contexto *online*. También se hizo esta declaración en una de las últimas iniciativas que se han promovido para debatir sobre el gobierno de internet, el *Netmundial* o *Global Multistakeholder Meeting on the Future of internet Governance*, que tuvo lugar en Brasil el 23 y 24 de abril de 2014, con ocasión de la celebración de los 25 años de vida de la *world wide web*. La reunión fue promovida por el Comité Gestor de internet en Brasil (CG.br) y /1Net, un foro que reúne a las entidades multisectoriales que participan en la gestión de internet. En la reunión participaron representantes de un gran número de países y organizaciones y se recibieron 188 aportaciones, provenientes de 46 países distintos. Como resultado de la reunión se emitió un documento en

Además, es preciso garantizar la neutralidad y el acceso libre a Internet, que se fundamenta en el acceso, por parte de los ciudadanos, a los servicios de comunicaciones electrónicas, de forma que sea un acceso en las mismas condiciones y sin distinguir según el tipo de servicio[1325]. En este sentido, se deben evitar prácticas que puedan poner en peligro los mencionados derechos de los usuarios[1326]. Así se ha reconocido, en el ámbito de la UE, con la aprobación, en 2015, de la reforma de la regulación en materia de telecomunicaciones[1327]. Con esta reforma, se ha introducido el derecho de los usuarios "a acceder y distribuir información y contenido, a utilizar y proveer aplicaciones y servicios, y a utilizar los equipos terminales que elijan, independientemente de la ubicación del usuario o del proveedor, del origen o destino del servicio, información o contenido, a través de su servicio de acceso a Internet"[1328].

---

el que se plasmaron los principios que debían regir el gobierno de internet y una hoja de ruta para la evolución futura del gobierno. *Netmundial multistakeholder statement*, 24 de abril de 2014, http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf (fecha consulta: 19.10.2014).

[1325] A raíz de la Declaración de la Comisión sobre la neutralidad de Internet (DO 2009/C 308/2), el 30 de junio de 2010, la Comisión Europea inició una consulta pública sobre "La Internet abierta y la neutralidad en Europa" y elaboró un informe (*Report on the public consultation on The open Internet and net neutrality in Europe, 9 november 2010, European Commission Information, Society and Media Directorate-General*) en el que, si bien no se señalaban problemas graves, en función de las 318 respuestas recibidas de diferentes partes interesadas, el *Body of European Regulators for Electronics Communications (BEREC)* señalaba algunas cuestiones que se habían presentado en algunos países miembros como el bloqueo o cobro adicional por servicios de voz a través del protocolo de Internet (VoIP) en Austria, Croacia, Alemania, Italia, Países Bajos, Portugal o Rumanía o los problemas planteados con el peer-to-peer (P2P) en Francia, Grecia, Hungría, Lituania, Polonia y el Reino Unido. Tras la consulta, la Comisión emitió la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre "La Internet abierta y la neutralidad de la red en Europa", COM(2011) 222 final, 19.4.2011.

[1326] En repuesta a la Comunicación mencionada sobre la neutralidad en Internet, el Supervisor Europeo de Protección de Datos emitió un dictamen en el que se destacaban las prácticas de inspección y supervisión que llevan a cabo algunos proveedores de la sociedad de la información y que podían vulnerar la neutralidad de Internet, la confidencialidad de las comunicaciones y la protección de los datos personales y la intimidad de los usuarios. Dictamen del Supervisor Europeo de Protección de Datos sobre la neutralidad de la red, la gestión del tráfico y la protección de la intimidad y los datos personales, DO 2012/C 34/01.

[1327] El Consejo de la UE informaba el 8 de julio de 2015 de la aprobación del proyecto de Reglamento de reforma de las principales normas reguladoras del sector de las telecomunicaciones. http://www.consilium.europa.eu/es/press/press-releases/2015/07/08-roaming-charges/ (fecha consulta: 22.8.2015).

[1328] Traducción de la autora, del artículo 3.1, del borrador final del Reglamento que se reproduce: "*Article 3. Safeguarding of open internet access. 1. End-users shall have the right to access and distribute information and content, use and provide applications and services and use terminal equipment of their choice, irrespective of the end-user's or provider's location or the location, origin or destination of the service, information or content, via their internet access service." Note from General Secretariat of the Council to Permanent Representatives Committee on the Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012, Interinstitutional File: 2013/0309 (COD), Council of the EU, Brussels, 8.7.2015.*

1.1.2. Del todo vale para mantenernos seguros a la indignación por el espionaje masivo

Como ya se comentó en este trabajo, especialmente a causa de los ataques terroristas del 11S, en 2001 en EEUU y, posteriormente, en 2004 en Madrid y en 2005 en Londres, se aumentaron las medidas que antepusieron la seguridad, a los derechos de los ciudadanos, más proclives a soportar este sacrificio[1329]. Entre estas medidas, la UE, en la línea de lo pautado por el Convenio de cibercriminalidad, aprobó una Directiva sobre la conservación de datos de las comunicaciones electrónicas, por parte de los prestadores de telecomunicaciones, con el fin de poderlos poner a disposición de las autoridades para luchar contra el terrorismo[1330].

El GA29 criticó la adopción de estas medidas que se adoptaron, con carácter urgente, para luchar contra el terrorismo y alertó de su incidencia a largo plazo en los derechos de las personas[1331].

La alarma social que originó el conocimiento, en 2013, de los programas de espionaje que había llevado a cabo el gobierno estadounidense, generó la necesidad por parte de la ciudadanía de transparencia respecto a la actividad de los poderes públicos. Se incentivó la percepción de que no existía posibilidad de preservar los derechos a la intimidad y a la protección de datos en el entorno digital, frente a las capacidades que otorgaba la tecnología a los poderes públicos para la supervisión masiva de sus ciudadanos.

Esta preocupación social, obligó a los gobiernos, y especialmente a la UE, a adoptar una postura crítica frente al tratamiento que el gobierno de los EEUU había efectuado de los datos de los europeos en sus programas. La Comisión Europea planteó

[1329] Ver Capítulo I.

[1330] Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15.3.2006, sobre conservación de datos generados o tratados en relación con la prestación de servicios de comunicación electrónica de acceso público o de redes públicas de comunicaciones, DO L 101 de 13.4.2006.

[1331] Entre otras medidas, el GA29 criticaba la definición demasiado amplia de infracciones en el Convenio de cibercriminalidad, la medida de conservación previa y generalizada de datos de comunicaciones electrónicas por parte de los prestadores de estos servicios y el intercambio de datos personales para distintos fines relacionados con la seguridad, especialmente si se realiza una comunicación prematura. Dictamen 10/2001 relativo a la necesidad de un enfoque equilibrado en la lucha contra el terrorismo, 0901/02/ES/Final WP 53, 14.12.2001, Grupo de trabajo Artículo 29 sobre la protección de datos, págs. 2 a 3.

una serie de actuaciones para poder restaurar la confianza perdida en las transmisiones de datos de la UE a los EEUU. Una de estas actuaciones fue la revisión de la Decisión *Safe Harbour*[1332].

En este contexto, el TJUE declaró, en 2014, la invalidez de la Directiva de conservación de datos[1333]. En el momento de aprobación de esta directiva, en 2009, ya se había cuestionado la idoneidad de su base jurídica, que se refería al primer pilar comunitario, ya que su materia, la conservación de datos para utilizarlos en la persecución de delitos, parecía pertenecer al tercer pilar -el correspondiente a la cooperación policial y judicial en materia penal-[1334]. No obstante, el TJUE había estimado que la base jurídica era acertada.

En la sentencia de 2014, sin embargo, el TJUE consideró que la directiva constituía una injerencia especialmente grave en los derechos a la vida privada y a la protección de datos de carácter personal. El TJUE recalcó, en su sentencia, el hecho de que la conservación y el uso posterior de los datos se efectuaran, sin que el ciudadano fuera informado y que podía generar, en este ciudadano, el sentimiento de que su vida privada era objeto de una vigilancia constante. Al analizar si la injerencia respetaba los requisitos establecidos por la Carta UE, el TJUE consideró que no se cumplía con el principio de proporcionalidad[1335].

[1332] *Restoring trust in EU-US data flows-Frequently Asked Questions, European Commission MEMO/13/1059, 27.11.2013, Brussels*. http://europa.eu/rapid/press-release_MEMO-13-1059_es.htm, (fecha consulta: 2.11.2014).

[1333] Sentencia del TJUE de 8 de abril de 2014, *Digital Rights Ireland* y *Seitlinger* y otros, C-293/12 y C-594/12, EU:C:2014:238.

[1334] Irlanda interpuso un recurso de anulación ante el TJUE de esta directiva, por no haber sido adoptada sobre la debida base jurídica. El TJUE respondió negativamente y confirmó que la base jurídica de la directiva debía incluirse en el primer pilar ya que la regulación se centraba en lo que afectaba a la actividad comercial de los proveedores de servicios de comunicaciones electrónicas y no en la actuación de las autoridades nacionales competentes en materia represiva, habilitadas para utilizar los datos conservados. Sentencia del TJUE de 10 de febrero de 2009, *Irlanda/Parlamento Europeo y Consejo de la Unión Europea*, C-301/06, EU:C:2009:68. Asimismo, surgieron críticas referidas a la falta de proporcionalidad. M.G. PORCEDDA, "Law enforcement in the clouds: is the EU data protection legal framework up to the task?" S. GUTWIRTH, R. LEENES, P. DE HERT, Y. POULLET (Ed.), VVAA, *European Data Protection: in good health?* Springer, Netherlands, 2012, pág. 218.

[1335] Hay que recordar que el artículo 52.1 de la Carta UE establece que cualquier limitación del ejercicio de los derechos y libertades reconocidos por la Carta UE debe ser establecida por ley, respetar el contenido esencial del derecho y respetar el principio de proporcionalidad. Hay que decir que el TJUE invalidó esta Directiva de conservación de datos, por lo que serán los órganos jurisdiccionales nacionales los que deberán interpretar sus normativas nacionales, a la luz de esta sentencia, para ver si se cumple o no el principio de proporcionalidad. Entiendo que el legislador europeo debería aprobar una norma que garantizara una persecución efectiva de los delitos, al mismo tiempo que protegiera adecuadamente los derechos de los ciudadanos. Es necesario conseguir el equilibrio, ya que el hecho de no contar con estos datos podría

Asimismo, otra reacción al espionaje fue la del Consejo de Derechos Humanos, de Naciones Unidas que autorizó, el 26 de marzo de 2015, la designación de un relator especial sobre el derecho a la privacidad que deberá realizar un primer informe sobre este derecho en la era digital[1336].

1.2. La tecnología como motor económico en un contexto de crisis global

Ante un contexto de crisis económica, la UE lucha por competir con EEUU, cuyas empresas tecnológicas, se han hecho con el mercado. Esto hace que deban equilibrarse estos intereses económicos con una protección del derecho a la protección de datos que, como ya vimos, difiere en ambos modelos jurídicos.

La Comisión Europea puso en marcha en 2010 la estrategia Europa 2020 para salir de la crisis y preparar la economía de la UE para los retos de esta década[1337]. Una de las siete iniciativas, que se incluyeron en esta estrategia fue la Agenda digital, que pretendía maximizar el potencial económico y social de las tecnologías de la información y la comunicación, como soporte esencial de la actividad económica y social[1338]. En 2015, la

considerarse como un incumplimiento de las obligaciones positivas, que tienen los Estados de asegurar la protección de los derechos de sus ciudadanos, de acuerdo con lo establecido por la jurisprudencia del TEDH, ver entre otras, sentencia del TEDH de 2 de marzo de 2009, *K.U. v. Finland*, apdo. 46. En esta sentencia se indica que aunque se tipifique una infracción si no se puede identificar al infractor y llevarlo ante la justicia, la protección tendría efectos limitados.

[1336] Alemania y Brasil presentaron un Proyecto de resolución a la Asamblea General de Naciones Unidas sobre "El derecho a la privacidad en la era digital", el 1 de noviembre de 2013, Sexagésimo octavo período de sesiones, Tercera Comisión, Tema 69b) del programa. Promoción y protección de los derechos humanos: cuestiones de derechos humanos, incluidos otros medios de mejorar el goce efectivo de los derechos humanos y las libertades fundamentales, A/C.3/68/L.45. Esta resolución pretendía alertar sobre el incremento de la capacidad de gobiernos y empresas de vigilar, interceptar y recopilar datos, lo que podía suponer una violación de derechos humanos y, especialmente, del derecho a la privacidad. En este texto se indicaba que los derechos de las personas también debían estar protegidos en Internet y se exhortaba a los Estados a que los respetasen y que revisaran sus prácticas y legislación relativas a la vigilancia y la interceptación de comunicaciones. Se incentivaba asimismo la instauración de mecanismos nacionales de supervisión y se solicitaba a la Alta Comisionada de las Naciones Unidas, para los Derechos Humanos, que presentara un informe sobre la protección del derecho a la privacidad, en el contexto de la vigilancia. El 26 de marzo de 2015 se publicaba la noticia de la designación de este relator, http://www.un.org/spanish/News/story.asp?NewsID=31995#.Va_V-N-JhMs (Fecha consulta: 22.7.2015).

[1337] Comunicación de la Comisión, Europa 2020: Una estrategia para un crecimiento inteligente, sostenible e integrador, COM(2010) 2020 final, Bruselas, 3.3.2010.

[1338] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Una agenda digital para Europa, COM(2010) 245 final/2, de 26.8.2010.

Comisión presentó su estrategia para conseguir un mercado único digital, uno de los puntos de la Agenda digital[1339].

En este documento se establecían tres pilares para lograr ese objetivo: mejorar el acceso de los consumidores y empresas a los bienes y servicios en línea, en toda Europa; crear las condiciones adecuadas para que las redes y servicios digitales prosperen; y aprovechar, al máximo el potencial de crecimiento de la economía digital, lo que requiere inversión en infraestructuras y tecnologías, como el *cloud computing* o el *big data*[1340]. Asimismo, entre los aspectos clave se mencionaba la adopción de medidas legislativas, como las relativas a la protección de datos[1341].

1.2.1. Nuevos modelos de negocio: de la industrialización de la tecnología mediante el cloud computing a la movilidad ilimitada

A principios del siglo XX, las industrias empezaron a desmantelar sus generadores y sus molinos de agua, ya que aparecieron los proveedores de energía eléctrica, de modo que ya no era necesario disponer de un generador propio, sino que se podía consumir electricidad en función de las propias necesidades. Estos nuevos proveedores construyeron centrales eléctricas y crearon redes por todo el territorio al que aprovisionaban. Del mismo modo ha sucedido con la tecnología[1342].

En un primer momento, las organizaciones invertían en sistemas informáticos que instalaban en sus propias ubicaciones. Sin embargo, posteriormente, diversos factores,

[1339] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, COM(2015) 192 final, Bruselas, 6.5.2015.
[1340] *Ibídem*, pág. 4.
[1341] Así lo manifestaba Jean-Claude Juncker, presidente de la Comisión Europea en sus directrices políticas para la próxima Comisión Europea, el 15 de julio de 2014. Estimaba que se podían generar hasta 250.000 millones de euros de crecimiento adicional en Europa durante su mandato, mediante ese mercado único digital. Pero, para ello, afirmaba que era necesario "tener el valor de abrir los compartimentos nacionales de regulación de las telecomunicaciones, de derechos de propiedad intelectual y de legislación sobre protección de datos, de gestión de las ondas de radio y de aplicación del derecho de la competencia". *Ibídem*, pág. 2.
[1342] Realiza esta comparación CARR. Este visionario vaticinaba, en el año 2005, la ineludible evolución hacia la tecnología, como un servicio que brindarían proveedores y no como un coste fijo destinado a pagar costosos sistemas informáticos propios, al igual que había sucedido con la energía eléctrica a finales del siglo XX. En ese momento, las empresas ya habían empezado a alojar su información en servidores de proveedores externos pero no se había llegado al punto en el que estamos ahora, en el que estos servicios han llegado a todo el público y permiten soluciones totalmente adaptables a las necesidades de los clientes. N. G. CARR, "The end of corporate computing", *MIT Sloan management review*, April, 2005. http://sloanreview.mit.edu/article/the-end-of-corporate-computing/ (fecha consulta: 9.9.2014).

como el aumento de velocidad de comunicación en Internet y de la capacidad de almacenamiento de información, propiciaron que empresas que habían invertido en grandes centros de datos, decidieran convertirse en proveedores de servicios de alojamiento de información en estas instalaciones[1343].

De esta forma, las organizaciones que decidieron optar por estos servicios podían prescindir de los costes que suponía el mantenimiento de un sistema propio y adaptar los servicios informáticos a sus necesidades. Los proveedores de este tipo de servicios podían ser muy competitivos, ya que ubicaban sus centros de datos en lugares donde les era más económico la instalación de los mismos y utilizaban servicios de mantenimiento que podían hallarse también en otros países donde fueran más asequibles. Estos nuevos servicios se bautizaron como *cloud computing* (computación en la nube).

a. La definición "oficial" de lo que se considera *cloud computing*

Con el fin de aproximarnos a lo que es el *cloud computing* se suele acudir a la definición que elaboró el *National Institute of Standards and Technology* (NIST)[1344]. En este documento se describe al *cloud computing* como un modelo de prestación de servicios tecnológicos, que permite el acceso previa demanda, desde cualquier lugar, a través de la red, a un conjunto de recursos informáticos compartidos y configurables (como redes de comunicación, servidores, capacidad de almacenamiento, aplicaciones informáticos y servicios), que pueden ser rápidamente suministrados con un mínimo esfuerzo o mínima intervención del proveedor[1345]. En este documento se diferencian tres

[1343] Ejemplo de ello son empresas como *Google* o *Amazon*. No es que esta posibilidad de alojar datos en servidores de terceros fuera un servicio nuevo, ya que desde el inicio de Internet ya se habían ofrecido servicios de alojamiento de páginas web, servicios de *housing* (mediante los que se podía alquilar un servidor o una parte del mismo) o servicios de utilización de programas informáticos que se hallaban alojados en los servidores del proveedor de servicios (los conocidos como *asp* o *application service provider*, proveedor de servicios de aplicaciones). Sin embargo, los factores apuntados relativos a la velocidad y capacidad de almacenamiento hacen que estos servicios vayan más allá, como se apuntará a continuación.

[1344] P. MELL, T. GRANCE, *The NIST definition of cloud computing, Recommendations of the National Institute of Standards and Technology, Special Publication 800-145 September 2011, NIST, U.S. Department of Commerce*. La denominación de *cloud computing*, es decir, computación en la nube deriva de la manera en la que se ilustra Internet en los diagramas de arquitectura de sistemas informáticos, en los que se representa Internet mediante una nube.

[1345] Las características esenciales de este servicio, según este documento son: el auto aprovisionamiento previa solicitud (*on demand self-service*); el acceso a través de una red (*broad network access*), que permite que desde cualquier dispositivo se pueda conectar; la puesta en común de recursos (*resource pooling*) que permite poner a disposición de los usuarios una multitud de recursos físicos y virtuales que se asignan de forma dinámica; la elasticidad (*rapid elasticity*) de forma que el suministro es automático y rápidamente

tipos de modalidades de servicio de *cloud computing* y cuatro modelos de desarrollo de los mismos[1346]. Es importante diferenciar estas formas de prestar los servicios, ya que tiene consecuencias a nivel jurídico.

Las modalidades de servicios, que se distinguen, son el software como servicio, (*Software as a Service* o SaaS)[1347], la infraestructura como servicio (*Infrastructure as a Service* o IaaS)[1348] y la plataforma como servicio (*Platform as a Service* o PaaS)[1349]. Según la modalidad de servicio de la que se trate, el control que tiene el cliente de la tecnología es mayor o menor, de forma que en la plataforma como servicio, el cliente tendrá el máximo control sobre la infraestructura, seguido de la infraestructura como servicio y, por último, estaría el software como servicio, respecto al que el cliente tendría la menor capacidad de control.

Respecto a los modelos de desarrollo de los servicios, se distingue si la nube es privada, pública, comunitaria o híbrida (*private cloud, community cloud, public cloud* o *hybrid cloud,* respectivamente). En la nube privada la infraestructura la utiliza una única organización y puede gestionarla ella misma, un tercero, o ambos. La nube comunitaria la utilizan una multitud de usuarios de distintas organizaciones, que tienen algún interés en común, y puede pertenecer o ser gestionada por una o más organizaciones de esta comunidad, por un tercero o por una combinación de estos. En la nube pública puede utilizar los servicios el público, en general, y puede pertenecer la infraestructura a empresas u otros tipos de organización (como universidades o administraciones públicas). La infraestructura en este caso estará en la ubicación del proveedor. La nube híbrida combinaría diversos de estos modelos (público, privado o comunitario).

---

escalable, según la demanda; servicio medido (*measured service*), de forma que se ajusta exactamente a las necesidades, ya que se puede monitorizar y medir exactamente el uso que se hace del mismo.

[1346] Además de estas modalidades, en el mercado han aparecido otras como la seguridad como servicio (*Security as a Service* o SecaaS) que ofrece los servicios precisos para la gestión de la seguridad de la organización.

[1347] En esta modalidad, el proveedor de servicios de *cloud computing* proporciona servicios que permiten a los usuarios el uso de programas informáticos alojados en la infraestructura del proveedor.

[1348] El proveedor de servicios de *cloud computing* proporciona la infraestructura para que el usuario aloje las aplicaciones que quiera y pueda gestionarlas, pero sin que pueda gestionar la infraestructura del proveedor que incluirá las redes, servidores, sistemas operativos o almacenamiento.

[1349] El proveedor de servicios de *cloud computing* ofrece las herramientas para que el usuario pueda desarrollar sus aplicaciones. El usuario no tendrá control sobre la infraestructura del proveedor aunque sí tendrá la posibilidad de gestionar los sistemas operativos, el almacenamiento, las aplicaciones y los componentes de comunicaciones. Se trata normalmente de una solución para empresas que necesitan desarrollar sus propias aplicaciones, o que son proveedores de servicios tecnológicos.

Evidentemente, la nube privada ofrecerá más garantías en cuanto a la seguridad y también en cuanto a cuestiones relacionadas con el cumplimiento legal, ya que podrá ser controlado por el cliente. Sin embargo, la nube privada conllevará mayores costes. La nube pública, por el contrario, implicará menor control por parte del cliente, pero conllevará un menor coste.

b. Desmontando la nube

Si bien hay que tener presente esta definición de *cloud computing* porque nos ayuda a clasificar de alguna manera los servicios de este tipo, hay que tener presente que el *cloud computing,* principalmente, surge como una manera de publicitar los servicios tecnológicos. Es más bien un concepto que ha contribuido al marketing de las empresas que ofrecen este tipo de servicios.

Por lo tanto, hay que relativizar el concepto y acercarse más bien a una tecnología cambiante que, cada vez permite mayores cosas, porque aprovecha las capacidades que brinda Internet. El *cloud computing* se focaliza en los servicios que aprovechan empresas o administraciones para externalizar los aspectos tecnológicos de sus organizaciones. Sin embargo, estos servicios se han extendido de tal forma que también los particulares los utilizan.

Otro tipo de servicios son las redes sociales, utilizadas ampliamente por los particulares, cuyos datos se alojan en los servidores de las compañías proveedoras que, a su vez, también pueden subcontratar servicios de *cloud computing*. De esta forma, la tecnología se aúna y todos los servicios se mezclan. Por ello, es necesario huir de un análisis jurídico estático y realizar el mismo, *a priori,* con un enfoque general, que luego deberá adaptarse al caso concreto. Hay que destacar, en este sentido, la labor del GA29 que analiza en sus dictámenes las novedades tecnológicas que el mercado va ofreciendo.

c. La movilidad y los objetos interconectados

Los datos personales pueden viajar y almacenarse en servidores que se hallan ubicados en cualquier parte del mundo. Esto permite que el usuario pueda acceder desde cualquier parte y con cualquier tipo de dispositivo cliente. El aumento de las capacidades

de estos dispositivos portátiles hace que la información esté disponible, todo el tiempo, en cualquier parte.

Estos mismos dispositivos, además de servir para acceder a la información se convierten en fuentes de información sobre el usuario. De esta forma, los *smartphones* se dotan de múltiples sensores que captan imágenes, vídeos, datos de geolocalización o navegación. La irrupción de las *apps* (abreviatura de *applications*, aplicaciones), aplicaciones para dispositivos portátiles que sirven para proporcionar múltiples funcionalidades, implicó la utilización, en muchos casos, de los datos originados por los dispositivos (por ejemplo, una *app* que informa de los restaurantes que hay más próximos mediante la utilización de los datos de geolocalización del móvil).

Pero no sólo los *smartphones* o las *tablets* proporcionarán información, sino que se empiezan a adaptar elementos que llevamos habitualmente con nosotros, como unas gafas o el reloj, para generar también información que se pueda procesar. Es lo que se ha dado en llamar *wearable computing* (informática que se puede llevar). Esta tecnología permitirá, por ejemplo, que se incluyan sensores en unas zapatillas deportivas, en una pulsera o en una camiseta, de forma que estos objetos recojan información sobre una persona, mientras hace ejercicio físico. Estos datos se volcarán en Internet y podrán ser procesados para obtener valores que pueden derivar en información sobre la salud. Esta tendencia se ha conocido como *quantified self* (cuantificarse a sí mismo) y convierte a los usuarios en productores de datos[1350].

Los sensores se han empezado a incluir en otro tipo de objetos de nuestro hogar, como las neveras, las cafeteras, las bombillas[1351], los detectores o las lavadoras. De esta forma, los sensores permiten obtener información de cualquier aparato e indirectamente

[1350] *Unlocking the value of personal data: from collection to usage, World Economic Forum, February 2013*,http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf (fecha consulta: 7.3.2015), pág. 8.

[1351] Un ejemplo de la importancia de esta tecnología es la de los sistemas de contador inteligente que ya son una realidad y que permiten transmitir el consumo de energía real, lo que se ha erigido en una de las piezas básicas para la construcción de políticas energéticas a nivel de la UE. De hecho, en función de los diferentes dictámenes del GA29 y los riesgos evidentes para los datos personales, la Comisión se ha avanzado a la aprobación del Reglamento en preparación y ha establecido que los Estados miembros animen a los responsables del tratamiento a aplicar un modelo de evaluación del impacto sobre la protección de datos que se ha elaborado *ad hoc* para redes inteligentes y para sistemas de contador inteligente y a tener en cuenta las recomendaciones del GA29. Recomendación de la Comisión de 10 de octubre de 2014 relativa al modelo de evaluación del impacto sobre la protección de datos para redes inteligentes y para sistemas de contador inteligente, DO L 300 de 18.10.2014.

de quienes los utilizan. En definitiva, la utilización de sensores en objetos es ilimitada y, en general, se ha llamado a esta tendencia *Internet of things* (Internet de las cosas). Esta tecnología permite mejorar la eficiencia en el suministro de servicios, como el de la energía eléctrica con los lectores inteligentes (*smart metering*). Asimismo, permiten mejorar la gestión de las ciudades (lo que se ha bautizado como *smart cities*).

Sin embargo, la aparición de todas estas tecnologías se fundamenta en las posibilidades permitidas por la conexión a Internet y el *cloud computing*. Es la posibilidad de contratar este tipo de servicios lo que ha permitido que nazcan otros modelos.

1.2.2. Los datos como materia prima: encontrando la aguja en el pajar

Toda esta explosión de información que se puede volcar a Internet de las diferentes fuentes que se identificaban en el punto anterior ha hecho que se hable de *big data* (datos masivos). Y no sólo confluyen en Internet los datos indicados, sino que también, con el propósito de que se exploten, las administraciones públicas publican datos, en lo que se conoce como *open data* (datos abiertos), con el fin de que esa información pueda ser utilizada por otras entidades y empresas para retroalimentar la economía. De esta forma, la reutilización de información se une a la necesidad de la administración de mejorar la eficiencia en su funcionamiento, mediante la utilización de medios electrónicos y a la urgente demanda de transparencia, exigida por los ciudadanos. La reutilización de los datos es lo que más gráficamente muestra el carácter de materia prima de los datos, que sirve para que empresas puedan fabricar otros productos.

Si bien, en un inicio toda esa información era inabarcable y desestructurada, han surgido herramientas que permiten su manejo, de forma que se puede analizar y obtener resultados, que pueden guiar la actuación de empresas y organizaciones[1352]. De esta forma, se puede decir que ahora es posible encontrar la aguja en el pajar[1353].

[1352] En un informe elaborado por La Casa Blanca sobre *big data*, se indica que se estima que en el año 2013 se generaron 4 Zettabytes de datos en todo el mundo. 1 Zettabyte son 1.000.000.000.000.000.000.000 bytes, por lo que se indica como ejemplo que se podría incluir en 1 Zettabyte las fotos que hicieran todos los estadounidenses durante 1 mes, haciendo una foto cada segundo. *Big Data: seizing opportunities, preserving values, Executive Office of the President, The White House, op. cit.*, pág. 2.
[1353] *Ibídem*, pág. 6.

Responsables del sector público y del sector privado, han empezado a utilizar esta tecnología. Así, una empresa puede analizar el comportamiento de los internautas que navegan por su sitio web, para conocer mejor el perfil de sus potenciales clientes. Un empleador puede analizar los datos que están en Internet para evaluar a un candidato. La policía puede analizar los datos, que obran en sus bases de datos y sumarlos a los que se encuentran en Internet para crear patrones de conducta y poder adelantarse a los actos de los potenciales delincuentes[1354].

Los intereses de ambos sectores, público y privado, confluyen, para sacar aún más partido a esta información. Las empresas obtienen datos de las administraciones pero, también éstas extraen información de las empresas, por ejemplo, cuando la policía accede a los sistemas de videovigilancia de las empresas de seguridad[1355].

Para analizar los datos se elaboran algoritmos que automáticamente procesan la información. De esta forma, ya no es el dato lo que el responsable valorará, sino la información tratada y filtrada por este algoritmo informático que, en definitiva, ha desarrollado alguna persona, en función de unos criterios subjetivos. La programación de estos algoritmos se mantiene oculta, debido a su importante valor comercial[1356]. En este sentido, ya se oyeron críticas acerca del algoritmo utilizado por *Google* en su motor de búsqueda, para personalizar los resultados, acerca de la selección de la información y la

[1354] Así se pueden mencionar ejemplos reales de la utilización de estos métodos. En Chicago, tras una oleada de asesinatos protagonizados por bandas se inició un proyecto piloto, mediante el que se analizaron los datos con los que contaba la policía y de otras fuentes, con lo que se consiguió una lista de 400 individuos que se estimó tenían una alta probabilidad de verse involucrados en un crimen violento. La policía de Filadelfia también utilizó un *software* para predecir qué personas en libertad condicional eran más proclives a cometer otra vez un delito, de forma que se pudiera reforzar su supervisión. *Big Data: seizing opportunities, preserving values, Executive Office of the President, The White House, op. cit.*, pág. 31.

[1355] La legislación española permite, en caso de peligro real para la seguridad pública o para la represión de infracciones penales, el acceso, por parte de las Fuerzas y Cuerpos de Seguridad, a los sistemas de seguridad instalados por las empresas de seguridad privada, de forma que puedan comprobar informaciones en tiempo real. Asimismo, se establece que la comunicación por parte de las empresas o personal de seguridad privada de información a las Fuerzas y Cuerpos de Seguridad, con la finalidad indicada, no constituirá vulneración de restricciones sobre divulgación de información impuestas por vía contractual o legal. (art. 15 Ley 5/2014, de 4 de abril, de seguridad privada, BOE núm. 83 de 5.4.2014).

[1356] Hay que recordar, en este sentido, cuando se comentaba la regulación del derecho de acceso en la Directiva 95/46/CE, que permitía acceder a la lógica utilizada en el tratamiento. Las empresas dedicadas al marketing presionaron para incorporar el Considerando 41 que garantizara que no iba a ser necesario entregar la información de los programas informáticos que pudiera estar protegida por el secreto comercial o la propiedad intelectual.

posible distorsión de la realidad[1357]. Incluso se han planteado procedimientos en contra del buscador por denuncias en las que se alega que favorece con el uso del algoritmo a sus servicios[1358]. Hay quienes alertan sobre el uso de los algoritmos y reclaman abordar las cuestiones éticas que debería plantear este uso[1359].

El uso de estos métodos cuestiona procesos, que permitían excluir la aplicación de la normativa, como el de anonimizar los datos. Datos que, en principio, no tenían porque identificar a una persona concreta, pueden llegar a hacerlo[1360]. Asimismo, las medidas técnicas tradicionales de protección, como el control de acceso o el cifrado, quedan superadas ante un mundo digital abierto a todo el mundo y que, gracias a la evolución tecnológica, puede ser aprehendido mediante herramientas de minería de datos[1361]. Como hemos visto, los mismos usuarios son productores de datos ¿Cómo proteger la información si está al alcance de cualquiera? ¿Cómo evitar que esa información perjudique a las personas, cuando son esas mismas personas quienes la generan?

Y es que la utilización de estas técnicas conlleva el riesgo de ocasionar vulneraciones en los derechos de los individuos y, especialmente, efectos

[1357] En este sentido, se ha alertado de la posible limitación en la obtención de información relevante a través de la personalización que proporcionan los buscadores. Se ha mostrado que usuarios diferentes ubicados en sitios diferentes obtienen resultados diversos, que pueden condicionar su percepción de lo que sucede en el mundo, de forma que se ilustra con la imagen de estar en el interior de una burbuja. Conferencia TED de E. PARISIER *Beware online "filter bubbles"*, http://www.youtube.com/watch?v=B8ofWFx525s (fecha consulta: 27.10.2014).

[1358] A inicios de 2015, los medios se hicieron eco de la filtración de un informe de la *Federal Trade Commission* de EEUU al periódico *Wall Street Journal*. Este informe era el resultado de una investigación, llevada a cabo por esta organización, en la que supuestamente se concluía que *Google* utilizaba su algoritmo para manipular los resultados de las búsquedas, de forma que se daba preeminencia a los productos de la compañía frente a los de los competidores. C. W. STREET, "*FTC leak suggests Google searches are biased, discriminatory"*, *Breitbart California*, 21.3.2015, http://www.breitbart.com/california/2015/03/21/ftc-leak-suggests-*Google*-searches-are-biased-discriminatory/ (fecha consulta: 8.4.2015) y R. JIMÉNEZ CANO, "*Google*, acusado de manipular los resultados del buscador", *El País Economía*, 22.3.2015, http://economia.elpais.com/economia/2015/03/21/actualidad/1426913017_935765.html (fecha consulta: 8.4.2015).

[1359] H. TAVANI, "Search engines and Ethics", E. N. ZALTA (Ed.), The *Stanford Encyclopedia of Philosophy*, Spring 2014 Edition, http://plato.stanford.edu/archives/spr2014/entries/ethics-search/ (fecha consulta: 23.8.2015). Asimismo, la asociación *Electronic Privacy Information Center* (EPIC) proclama la necesidad de la transparencia de los algoritmos, en una iniciativa denominada "*Algorithmic transparency: end secret profiling*", mediante la que denuncia usos que considera inapropiados en https://epic.org/algorithmic-transparency/.

[1360] *Ibídem*, pág.8.

[1361] D.J. WEITZNER, H. ABELSON, T. BERNERS-LEE, J. FEIGENBAUM, J. HENDLER y G.J. SUSSMAN, "Information Accountability," *Communications of the ACM*, June 2008, Vol. 51, Nº 6, pág. 82.

discriminatorios[1362]. Sin embargo, el análisis de todos estos datos que se vuelcan en Internet ofrece un sinfín de posibilidades de innovación, en todos los campos que se puedan imaginar, en un contexto de crisis económica global[1363]. Por eso, es necesario encontrar el equilibrio entre las posibilidades de innovación, que permite esta tecnología y los riesgos que puede acarrear para los derechos de las personas.

2. EL CONCEPTO DE RESPONSABLE: DEBILIDADES Y FORTALEZAS ANTE EL DESAFÍO DIGITAL

Para exponer las debilidades y fortalezas del concepto del responsable, me centraré en dos supuestos que han generado, como se ha expuesto anteriormente, algunas tensiones en la figura: los servicios de *cloud computing* y la determinación de la responsabilidad de un servicio de búsquedas en el asunto *Google*[1364]. Por tanto, a la hora de analizar ambos supuestos hay que tener en cuenta que se realizará, en el caso del *cloud computing*, una aproximación más general y, en el caso del servicio de búsquedas se podrá entrar en más detalle, al suponer un ejemplo concreto de la aplicación del concepto.

Del análisis de ambos supuestos se puede adelantar ya una conclusión sobre estas debilidades y fortalezas del concepto de responsable. La fortaleza del concepto es su existencia misma. El hecho de contar con este rol, que incluye unos elementos, que si se cumplen, activan la responsabilidad del sujeto, es en sí mismo, una fortaleza, porque persigue la seguridad jurídica respecto a los factores en los que la figura es clave y que se abordaron anteriormente en este trabajo. Ahora bien, la debilidad sería la utilización del concepto, de forma que si no se realiza correctamente el análisis, puede llevar al efecto contrario al deseado, es decir, a la inseguridad jurídica.

[1362] Un ejemplo para ilustrarlo es el algoritmo utilizado por unos supermercados para ofrecer ofertas a sus clientes en Internet. A raíz de los valores que se tenían en cuenta en el algoritmo, como la distancia a la que se encontraban otras tiendas competidoras, finalmente resultó que por el mismo producto se ofrecían menos descuentos a las personas que estaban ubicadas en zonas más desfavorecidas. J. VALENTINO-DEVRIES, J. SINGER-VINE, A. SOLTANI, *Websites vary prices, deals based on user's information, The Wall Street Journal*, 24.12.2012. http://online.wsj.com/articles/SB10001424127887323777204578189391813881534, (fecha consulta: 30.11.2014). En este sentido, La Casa Blanca emitió en febrero de 2015 otro informe sobre *big data*, pero esta vez centrado en la discriminación de precios y alertaba de la necesidad de someter a escrutinio continuo el análisis del big data para usos comerciales, especialmente si las empresas utilizan información sensible de forma no transparente.

[1363] No en vano el informe que realizó La Casa Blanca sobre *big data* se titulaba aprovechando oportunidades, preservando valores (*Big Data: seizing opportunities, preserving values*). *Big Data: seizing opportunities, preserving values, Executive Office of the President, The White House, op. cit.*.

[1364] *Ibídem*. Este asunto ha sido conocido porque el TJUE se ha pronunciado sobre el conocido como "derecho al olvido".

2.1. ¿Una inadecuada atribución de responsabilidad en los servicios de *cloud computing*?

De acuerdo con el estudio que se ha realizado del concepto de responsable del tratamiento, se analizarán los diferentes elementos que lo configuran, en el entorno del *cloud computing*, de forma que pueda determinarse quién debe considerarse responsable. El análisis se realiza en función del concepto establecido en la Directiva 95/46/CE y, en virtud, de los criterios que se sugirieron, al estudiarlo[1365]. Hay que recordar que estamos ante un concepto autónomo de derecho comunitario y que, pese a las divergencias apuntadas en las leyes nacionales europeas, debería interpretarse, de acuerdo con la Directiva 95/46/CE.

2.1.1. Elemento subjetivo

En la prestación de servicios de *cloud computing* tendremos como principales sujetos participantes al cliente y al proveedor de servicios. El cliente puede ser un usuario individual, un consumidor, o puede ser una empresa o una administración pública. El proveedor puede ser una única empresa o puede subcontratar a otras empresas y también puede ser una administración pública.

Respecto al elemento subjetivo del concepto, la definición de la Directiva 95/46/CE especificaba que podía ser responsable del tratamiento "la persona física o jurídica, autoridad pública, servicios o cualquier otro organismo" (art. 2.d) Directiva 95/46/CE). En el análisis realizado anteriormente, de este elemento, se concluyó que era muy amplio y podía incluir prácticamente todo tipo de organizaciones, tanto del sector público, como del sector privado. La identificación del sujeto en el entorno tecnológico tendrá la misma complejidad que en el entorno físico.

En principio, las partes deberían estar claramente definidas en la relación contractual. Sin embargo, pudiera ser que, quien se identifica en el contrato, no fuera realmente quien pudiera calificarse de responsable. Asimismo, aunque propugnemos que

[1365] Ver Capítulo II.

el concepto debe interpretarse, de forma respetuosa, con la Directiva 95/46/CE, hay que tener presentes las diferencias existentes en las leyes nacionales, que son las que deben aplicarse, de entrada. Por ejemplo, habrá que tener en cuenta si la legislación admite que puedan ser responsables las entidades sin personalidad jurídica (como la LOPD o la Ley polaca) o si podremos hacer responsable a un empleado o un funcionario (Ley irlandesa).

Este tipo de servicios son habitualmente multicapa, de forma que hay diversos prestadores implicados en la prestación del mismo. Lo realmente complejo es desentrañar qué sujetos están detrás de estas capas[1366], especialmente cuando la perspectiva, desde la que se realiza el análisis es la del cliente. Uno de los aspectos más importantes para poder cumplir con la normativa, en estos supuestos, será conocer exactamente los detalles del servicio que se contrata, con el fin de realizar un análisis jurídico correcto.

2.1.2. Elemento objetivo

El elemento objetivo supone analizar si debemos considerar que estamos ante un supuesto que entra dentro del ámbito de aplicación material de la normativa aplicable. El objeto al que se refiere la definición de responsable en la Directiva 95/46/CE es el tratamiento de datos personales. No obstante, si queremos evitar un conflicto con la ley nacional, habrá que tener en cuenta las divergencias entre las leyes nacionales que, al transponer la Directiva 95/46/CE, han contemplado diferentes objetos[1367].

Hay que resaltar, en el contexto del *cloud computing*, varias cuestiones que tienen especial relevancia a la hora de revisar el elemento objetivo: el concepto de datos personales y la posibilidad de considerar que estamos ante alguna de las exclusiones del ámbito de aplicación.

[1366] Por ejemplo, un servicio de *chat* de soporte, puede estar contratado a un tercero y, visualmente, aparecer totalmente integrado en el sitio web del servicio de *cloud computing*. El cliente tendrá la percepción de que el servicio se lo presta el proveedor con quien ha contratado, cuando en realidad, es otro sujeto quien lo lleva a cabo o quien presta su plataforma al proveedor principal. De hecho la integración de *apps* de terceros es algo que promueven servicios, como las redes sociales, con el fin de crear contenido adicional para sus usuarios. En ese caso habrá que analizar cómo se realiza esta integración y, especialmente, si se proporciona acceso a los datos de los usuarios.
[1367] Ver Capítulo III.

Respecto al concepto de datos personales, se ha planteado si se podían utilizar las técnicas para anonimizar, así como el cifrado y la fragmentación, como posibles vías de escape a la aplicación de la normativa[1368]. Si los datos que se proporcionan al proveedor de *cloud computing* no le permiten identificar ni hacer identificables a las personas titulares, entonces se tendría que considerar que no se aplicaría la normativa, porque no habría datos de carácter personal.

Sin embargo, hay que recordar las cautelas con las que deben valorarse estas medidas[1369]. El proceso de anonimato debería ser irreversible para el proveedor para que pudiera excluirse la aplicación de la legislación[1370]. En el caso de que el proveedor aplicara técnicas de cifrado o de fragmentación, el GA29 las considera equiparables al uso de pseudónimos, es decir, serían medidas de seguridad y no permitirían excluir la aplicación de la normativa[1371].

En lo que se refiere a las exclusiones del ámbito de aplicación, si el cliente de los servicios de *cloud computing* es una persona física que actúe como consumidor de los mismos, puede ser que proporcione datos propios y, por tanto, se le califique como titular de estos datos que tratará el proveedor de servicios. También puede ser que proporcione datos de terceros (por ejemplo de amigos, familiares o contactos). En este último caso, debe analizarse si esta persona física también debe considerarse responsable, respecto a estos datos que proporciona al servicio de *cloud computing*. Asimismo, en ambos casos, habrá que ver si el proveedor de servicios actúa como responsable o no.

Para ello, de forma previa, es necesario valorar si es posible aplicar la excepción contemplada en el ámbito de aplicación de la Directiva 95/46/CE relativa al ejercicio de actividades personales o domésticas (art. 3.2 Directiva 95/46/CE). De acuerdo con la

[1368] La fragmentación o dispersión de los datos, es una técnica que se utiliza en los servicios de cloud computing, que, sin aplicar el cifrado, pretende lograr un efecto similar. Consiste en fragmentar la información almacenada que se dispersan entre diferentes servidores. Si la dispersión se utiliza junto al cifrado se incrementa la seguridad. *Security guidance for critical areas of focus in cloud computing v3.0, Cloud Security Alliance, 2011*, https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf (fecha consulta: 22.8.2014), pág. 52.

[1369] Ver Capítulo II.

[1370] El GA29 además apunta a la sintonía en esta interpretación con normas internacionales de estandarización como la ISO 29100:2011. Dictamen 5/2014 sobre técnicas de anonimización, *op. cit.*, pág. 6.

[1371] Dictamen 5/2012 sobre la computación en nube, 01037/12/ES WP 196, 1.7.2012, Grupo de trabajo Artículo 29 sobre la protección de datos, pág. 17.

jurisprudencia del TJUE, no podrá incluirse en esta excepción un tratamiento de datos personales consistente en la difusión de estos datos por Internet, de modo que resulten accesibles a un grupo indeterminado de personas[1372].

Así, por ejemplo, en servicios como las redes sociales, donde los usuarios son personas físicas que puede ser que publiquen datos personales de otras personas, si esta publicación se realiza de forma que estos datos sean accesibles a un grupo indeterminado de personas, no podrán aplicar esta excepción de la Directiva 95/46/CE y, por tanto, se les podrá considerar responsables de tratamiento, si se cumplen los otros elementos del concepto[1373].

Respecto a los proveedores, en este supuesto, no podrían aplicar esta exclusión en ningún caso, ya que los fines que persiguen con el tratamiento de datos personales de sus usuarios no encajarían en este ejercicio de actividades familiares y domésticas[1374].

2.1.3. Elemento funcional

De acuerdo con el concepto de responsable de la Directiva 95/46/CE habría que determinar que sujetos de los que participan en un servicio de *cloud computing* tienen la capacidad de determinar los fines y los medios del tratamiento de datos personales y, por tanto, serán considerados responsables.

[1372] Sentencia del TJUE de 6 de noviembre de 2003, *Bodil Lindqvist*, C-101/01, EU:C:2003:596, apdo. 47. En su ámbito de aplicación la Ley italiana refleja la doctrina de esta sentencia, de forma que dispone su aplicación a los tratamientos de datos personales, que lleven a cabo personas físicas, para fines personales, si estos datos se van a comunicar de forma sistemática o si se van a difundir (art. 5.3 Ley italiana).

[1373] Así, el GA29 considera que un usuario de una red social podrá ser calificado como responsable del tratamiento, sin que pueda aplicarse esta excepción, cuando el usuario actúe, en nombre de una asociación o empresa o use la plataforma con fines comerciales, políticos o benéficos. En este caso, el hecho de tener un elevado número de contactos, puede ser una indicación de este tipo de uso. Otro supuesto en que también será considerado responsable será, cuando el usuario de acceso a su perfil, más allá de un reducido grupo de contactos seleccionados. Dictamen 5/2009 sobre las redes sociales en línea, 01189/09/ES WP 163, 12 de junio de 2009, Grupo de trabajo Artículo 29 sobre la protección de datos, pág. 6. Así lo indica también TRONCOSO REIGADA que destaca asimismo que la inclusión de datos de otras personas en un perfil personal con un número elevado de contractos o abierto a todos los usuarios de la red social sin restricciones de acceso o al público en general a través de motores de búsqueda implica una publicación de datos donde no es posible identificar al cesionario y que supone una cesión indiscriminada de datos. Especialmente grave será cuando lo que se comunique sean datos especialmente protegidos. A. TRONCOSO REIGADA, "Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales. Parte una" *IDP. Revista de Internet, Derecho y Política*, Número 15, pág. 72. UOC. http://idp.uoc.edu/ojs/index.php/idp/article/view/n15-troncoso/n15-troncoso-es (fecha consulta: 8.7.2015).

[1374] No sólo los servicios consistentes en redes sociales, sino también servicios tan populares como algunos de comunicación como *Whatsapp* o de almacenamiento como *Dropbox*. Ello sin perjuicio de las cuestiones que se tendrán que tener en cuenta relativas a la legislación aplicable en estos casos.

Parece claro que el cliente, por regla general, determinará los fines en este tipo de servicios, ya que a la pregunta de ¿por qué se realiza el tratamiento? se respondería que porque así lo ha decidido el cliente, que ha querido contratar ese servicio y que ha decidido entregar unos datos personales al proveedor. De acuerdo con la interpretación seguida del concepto, habría que entender que, por el hecho de determinar los fines, ya sería responsable. Si el proveedor decidiera utilizar los datos que el cliente le proporcione para una finalidad diferente a la prestación del servicio, también será considerado responsable.

En cambio a la pregunta de si el cliente determina los medios del tratamiento, la respuesta ya no parece tan obvia. Recordemos que el GA29 distinguía en los medios dos tipos de elementos. Así, los primeros, denominados elementos esenciales, que calificarían al sujeto de responsable, serían: los datos que se tratarán, las operaciones a realizar como la conservación y los terceros que tendrán acceso. Por otro lado, estarían los medios técnicos y organizativos, como el *software* o el *hardware* utilizados para el tratamiento, que no se considerarían, en principio, determinantes para calificar al responsable del tratamiento, sino que también podrían ser determinados por el encargado del tratamiento, sin activar su responsabilidad[1375].

Para poder valorar si el cliente es el que determina los elementos esenciales de los medios del tratamiento se puede acudir a la fuente de la que emana la capacidad de control, tal como sugería el GA29[1376].

La competencia legal será especialmente importante respecto a las administraciones públicas. Su actividad se ve limitada por el marco legal, lo que implicará que sea más difícil que pueda traspasar el control sobre los fines y los medios del tratamiento al proveedor[1377]. En la legislación española, que entiendo considera

[1375] Ahora bien, hay que recordar que, por ejemplo, en la Ley italiana la capacidad de decisión del responsable se proyecta sobre "la finalidad, la modalidad de tratamiento de datos personales y los instrumentos utilizados, incluido todo lo relativo a las medidas de seguridad" (art. 4.f) Ley italiana), por tanto, las medidas de seguridad se perfilan como algo esencial sobre lo que decide el responsable. También he considerado que las medidas de seguridad deben considerarse elemento esencial de los medios, en la legislación española.

[1376] Ver Capítulo II.

[1377] Como indica VALERO TORRIJOS, se establece en el artículo 33 Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (BOE núm. 150 de 23.6.2007) que "la gestión

elementos esenciales las medidas de seguridad, se añade a la normativa que regula el marco competencial, la específica regulación en materia de seguridad en la administración electrónica[1378].

Hay que añadir las situaciones en las que proveedores de estos servicios ubicados en otros países, son requeridos por las autoridades administrativas de los mismos a entregar información alojada en sus servidores de clientes europeos. Esta problemática que abordaré posteriormente, es especialmente sensible cuando los clientes sean administraciones públicas. Lo mismo sucede en caso de transferencias internacionales de datos que se puedan realizar, sin el conocimiento de los clientes. También parece que, en el caso de que estos clientes fueran administraciones adopta un especial cariz de gravedad.

Además de la competencia legal, en este escenario también tendrán especial relevancia la tipología del servicio contratado y las condiciones contractuales. Y es que, como indicamos la capacidad de control del cliente vendrá determinado por el tipo de servicio y el modelo de desarrollo del mismo. Estas diferencias se hacen patentes, de nuevo, en materia de seguridad de la información, aspecto clave en este tipo de servicios. Pese a que, como he indicado, las medidas de seguridad no son uno de los elementos esenciales de los medios, según el GA29, el mismo grupo destaca su importancia en este contexto. El GA29 recuerda la responsabilidad del cliente de velar para que el prestador de servicios cumpla con las medidas de seguridad[1379].

---

electrónica de la actividad administrativa respetará la titularidad y el ejercicio de la competencia por la Administración Pública, órgano o entidad que la tenga atribuida y el cumplimiento de los requisitos formales y materiales establecidos en las normas que regulen la correspondiente actividad". De esta forma, el proveedor de servicios de cloud computing no podrá, en última instancia, adoptar las decisiones que conlleven el ejercicio de las competencias administrativas. Esta cuestión es esencial cuando por ejemplo se desarrolle un servicio electrónico, en el que deba adoptarse una decisión administrativa. El diseño del mismo debe realizarse de forma que asegure que se cumplen todas las garantías legales. J. VALERO TORRIJOS, "La Administración Pública en la nube. Análisis de las implicaciones jurídicas desde la normativa sobre Administración electrónica", R. MARTÍNEZ MARTÍNEZ (Ed.), VVAA, *Derecho y cloud computing*, *op. cit.*, pág. 233.

[1378] Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, (BOE núm. 25 de 29.1.2010, Sec. I Pág. 8089) y el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (BOE núm. 25 de 29.1.2010, Sec. I Pág. 8139).

[1379] Artículo 17.2 Directiva 95/46/CE, Dictamen 5/2012 sobre la computación en nube, *op. cit.*, págs. 16 a 19.

El cliente tendrá mayor control sobre la seguridad de los datos, cuando contrate servicios de infraestructura (IaaS), menor en la contratación de servicios de plataforma (PaaS) y mucho más reducida en los servicios de *software* (SaaS)[1380]. Asimismo, en una nube privada, el cliente tendrá más control, que en una nube pública. De modo inverso, a menor capacidad de control del cliente, mayor será la capacidad de control del proveedor sobre la seguridad.

Otro elemento que nos ayudará en el análisis de la fuente de la que emana la capacidad de determinación del responsable, son las condiciones contractuales. El primer indicio será si se trata de unas condiciones pactadas *ad hoc* o unas condiciones generales. En el primer caso, obviamente, de entrada habrá un mayor equilibrio entre las partes que habrán podido negociar las cláusulas. En el segundo caso, existirá un desequilibrio en beneficio de quien las ha impuesto, el proveedor.

En cualquier caso, pese a estos indicios, habrá que analizar el contrato para establecer a que sujeto otorga el poder de determinar los fines y los elementos esenciales de los medios. Y es que, desde el año 2012, en el que se desarrollaron especialmente estos servicios de *cloud computing* y en el que se sitúan la mayoría de documentos de análisis jurídico de este fenómeno, se ha trabajado, tanto en el ámbito de las instituciones, como en el de los mismos proveedores, para intentar mejorar ese marco contractual[1381].

Estos trabajos, a nivel de las instituciones, no sólo han perseguido la mejora en la protección de datos, sino que también se han realizado para incentivar la utilización del *cloud computing*, como motor de la economía europea. En esta línea, la Comisión Europea creó un grupo de expertos que ha trabajado en la elaboración de contratos tipo para estos servicios y que ha tenido en cuenta los aspectos relativos a la protección de datos[1382].

[1380] R. MARTÍNEZ MARTÍNEZ, "El derecho y el cloud computing", R. MARTÍNEZ MARTÍNEZ (Ed.), VVAA, *Derecho y cloud computing, op. cit.*, pág. 29 y *Security guidance for critical areas of focus in cloud computing v3.0, Cloud Security Alliance, 2011, op. cit.*, pág. 22.

[1381] En este sentido se pueden señalar iniciativas de los proveedores como *Amazon* que permite al cliente seleccionar la zona donde quiere que se ubiquen sus datos. *Amazon Web Services, Whitepaper on EU data protection, april 2015, op. cit.*. Asimismo esta compañía y también *Microsoft*, como ya se señaló, han utilizado los nuevos mecanismos, con el fin de facilitar a sus clientes la tramitación necesaria frente a las autoridades de control para la realización de transferencias internacionales de datos. Ver Capítulos V y VI.

[1382] Ya se ha señalado que la promoción del uso del cloud computing estaba en uno de los pilares de la Agenda digital para desarrollar el mercado único digital. Entre las acciones concretas que se establecieron

No sólo habrá que analizar las condiciones contractuales, sino que habrá que acudir a la capacidad de influencia de hecho ¿Cómo se puede verificar quién ostenta realmente el control, pese a lo que establezca el contrato? Podrá acudirse a toda la información sobre el servicio, que podrá hallarse en la plataforma o en los manuales que se proporcionen al cliente, los apartados de ayuda o la información comercial. En muchos casos, será en esta información donde hallaremos realmente la respuesta a quién asume el control sobre fines y medios. Como han señalado las autoridades de control, los riesgos que conlleva el uso de estos servicios para la protección de datos, se pueden agrupar en la falta de información y de control sobre los datos[1383]. Sin duda, son dos aspectos que van unidos, de forma que si el servicio es opaco para el cliente, eso implicará forzosamente que no tenga el control.

Si el cliente no conoce las subcontrataciones que realiza el proveedor o ignora que el proveedor recoge ciertos datos de los empleados del cliente, al utilizar el servicio o desconoce el tipo de operaciones a las que somete los datos o el lugar donde se ubican los datos, no podrá ejercer su capacidad de determinación. Por ello, la transparencia en la forma en la que el proveedor desarrollará el servicio será primordial, como paso preliminar para poder establecer si puede existir esa capacidad de determinación. En definitiva, tras verificar si existe esta información, deberá analizarse la misma para concluir si la capacidad de determinación de fines y medios reside en el cliente o en el proveedor.

Sin embargo, la postura de las autoridades de protección de datos ha sido, principalmente, de simplificación, de forma que *a priori* se califica al cliente, como responsable y al proveedor de servicios de *cloud computing*, como encargado del tratamiento. La AEPD y el GA29 se han decantado por esta opción[1384]. De esta forma,

---

para promover ese uso estuvo la de elaborar unas "condiciones contractuales seguras y justas". Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Liberar el potencial de la computación en nube en Europa, COM(2012) 529 final, Bruselas, 27.9.2012, págs. 13 a 15.

[1383] Dictamen 5/2012 sobre la computación en nube, *op. cit.*, págs. 7 a 8 y *Working paper on cloud computing-Privacy and data protection issues, "Sopot Memorandum", International Working Group on Data Protection in Telecommunications, Sopot (Poland), 24.4.2012*, págs. 2 y 3.

[1384] La AEPD en los documentos que ha emitido para dar las pautas sobre el tema del *cloud computing* señala claramente a los clientes como responsables y a los proveedores como encargados del tratamiento. Guía para clientes que contraten servicios de *Cloud Computing*, Agencia Española de Protección de Datos,

han incidido en la responsabilidad del cliente, de su capacidad de elección del servicio. No obstante esta postura inicial y, entiendo que preventiva, de las autoridades, sin perjuicio de la clara responsabilidad del cliente, debe haber una coherencia en la aplicación del concepto del responsable. Si en función de las circunstancias de hecho, se determina que es el proveedor quien determina elementos esenciales de los medios, deberá calificarse de responsable[1385].

Hay que destacar algunas autoridades que han matizado la calificación. En este sentido mencionar a la autoridad de control francesa que ha considerado, de entrada, que el proveedor podrá ser calificado de responsable conjunto en estas situaciones en las que *de facto*, el cliente no tendrá capacidad de decidir[1386]. Entiendo que esta postura aún

---

op. cit., págs. 13 y 4 y Orientaciones para prestadores de servicios de Cloud Computing, Agencia Española de Protección de Datos, 2013, http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/ORIENTACIONES_Cloud.pdf, (fecha consulta: 23.9.2014), págs. 5 y 6. El GA29 ha dictaminado que el hecho de que el contrato lo elabore el proveedor del servicio y no el responsable del tratamiento no es por sí mismo base suficiente para concluir que el proveedor del servicio deba considerarse el responsable del tratamiento, en la medida en que el responsable ha aceptado libremente las condiciones contractuales y, por lo tanto, la plena responsabilidad sobre éstas. No se acepta que el desequilibrio en cuanto al poder contractual entre un pequeño responsable y un gran proveedor de servicios debiera considerarse una justificación para que el primero acepte unas condiciones que no se ajusten a la legislación de protección de datos. Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.*, pág. 29 y Dictamen 5/2012 sobre la computación en nube, pág.10.

[1385] En los supuestos normales de servicios de *cloud computing* donde un proveedor celebre contratos con sus clientes y les preste estos servicios mediante subcontratación de otras empresas RUBÍ NAVARRETE señala que no cabe duda que este proveedor tiene una importante capacidad para tomar decisiones sobre estos servicios. Puede seleccionar a sus subcontratados y optar por el lugar donde se producirá el tratamiento o delimitar las medidas de seguridad. El autor, sin embargo, considera que esta capacidad de decisión no excluye que los clientes sigan ostentando esta condición de responsables, por tanto, estima que, como punto de partida, el prestador de servicio debe considerarse encargado del tratamiento. J. RUBÍ NAVARRETE, "El proveedor de cloud como encargado del tratamiento", R. MARTÍNEZ MARTÍNEZ (Ed.), VVAA, *Derecho y cloud computing*, *op. cit.*, págs. 93 a 94. PORCEDDA, en cambio, plantea si es necesario considerar al proveedor de servicios de *cloud computing* como un responsable y no un encargado del tratamiento M.G. PORCEDDA, "*Law enforcement in the clouds: is the EU data protection legal framework up to the task?*", S. GUTWIRTH, R. LEENES, P. DE HERT, Y. POULLET (Ed.), VVAA, *European Data Protection: in good health?*, *op. cit.*, pág. 228.

[1386] Así, la CNIL estima que, aunque el esquema tradicional es el de que el cliente sea responsable y el proveedor sea encargado, en este tipo de servicios de *cloud computing*, sobre todo en los PaaS y SaaS públicos, queda patente que los clientes no pueden realmente decidir ni dar instrucciones que garanticen la efectividad de las garantías d seguridad y confidencialidad, que deben aportar los proveedores. Por ello, el proveedor podrá ser considerado *a priori* como responsable conjuntamente con el cliente, en virtud de la definición de responsable del tratamiento, que proporciona el artículo 2 Directiva 95/46/CE, ya que participa en la determinación de los fines y los medios de los tratamientos. Incluso la CNIL sugiere un reparto de responsabilidades formal entre ambos sujetos, de manera que, por ejemplo, la notificación de ficheros, la autoridad recomienda que la lleve a cabo el cliente, así como el deber de informar a los interesados. En cambio, la obligación de cumplir con las medidas de seguridad y confidencialidad, así como la de atender el ejercicio de derechos de los interesados, la autoridad recomienda que se repartan entre ambos sujetos. *Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing*, CNIL, 25.6.2012, págs. 5 y 6.

impone más barreras a este tipo de servicios, pero creo que jurídicamente es la más adecuada. Asimismo, el Supervisor Europeo de Protección de Datos también ha indicado que la complejidad técnica de este tipo de servicios puede implicar que el cliente no sea el único en determinar los fines y los medios del tratamiento[1387]. El Supervisor considera que, en este escenario, reflejará mejor la verdadera relación de poderes de cliente y proveedor, respecto al tratamiento, el supuesto de corresponsabilidad[1388].

Hay que añadir que, durante la elaboración del proyecto de Reglamento que sustituirá a la Directiva 95/46/CE, se abordó esta cuestión. La presidencia griega del Consejo de la UE insistió en que el desequilibrio que puede producirse en los servicios de *cloud computing*, por ser el proveedor una empresa de mayor envergadura, que la del cliente, no puede implicar que el cliente deje de tener responsabilidad respecto al cumplimiento de la normativa que debe reflejarse en las condiciones contractuales suscritas[1389]. Por eso, lo que sugería la presidencia, como solución a este problema, era la adopción de modelos de contratos que podrían utilizarse entre el cliente responsable y el proveedor encargado del tratamiento, al igual que se hace en las transferencias internacionales. De esta forma así se aseguraría que el contrato cumpliera efectivamente con lo establecido en la normativa de protección de datos[1390].

---

http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf, (fecha consulta: 23.9.2014).

[1387] Si bien el Supervisor realiza este análisis, en el marco del proyecto de Reglamento General de Protección de datos que sustituirá la Directiva 95/46/CE, entiendo que es perfectamente aplicable a la legislación vigente. El Supervisor indica que la determinación de los elementos esenciales de los medios no será siempre una prerogativa del cliente, ya que el proveedor habitualmente diseña, opera y mantiene la infraesctructura tecnológica, que puede incluir desde servicios esenciales de hardware y software (en el IaaS), la plataforma (en el PaaS) o las aplicaciones (SaaS). Como indica el Supervisor en los servicios de IaaS el cliente podría tener cierta capacidad de influencia en las condiciones del servicio pero en el SaaS resultaría claro que no tiene capacidad de control sobre los medios del tratamiento y debería ser calificado el proveedor como corresponsable. *Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", 16.11.2012*, pág 12.

[1388] *Ibídem*, pág. 13.

[1389] *Note from Presidency to Working Group on Information Exchange and Data Protection (DAPIX) on specific issues of Chapters I-IV of the General Data Protection Regulation-certain aspects of the relationship between controllers and processors. Interinstitutional file: 2012/0011(COD) 5345/14, Council of the EU, Brussels, 15.1.2014*, págs. 7 a 8 y *Note from Presidency to Working Group on Information Exchange and Data Protection (DAPIX). Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)-Article 26. Interinstitutional file: 2012/0011(COD) 5881/14, Council of the EU, Brussels, 31.1.2014.*

[1390] Incide también en la importancia del contrato suscrito en el ámbito del *cloud computing* PUYOL MONTERO. Este autor considera que la determinación de los niveles de responsabilidad es una asignatura pendiente en el desarrollo del *cloud computing* y que la función de los proveedores debe estar claramente delimitada de antemano, J. PUYOL MONTERO, *Algunas consideraciones sobre cloud computing, Premio*

En este sentido, señalar los trabajos ya mencionados, que pretenden mejorar las condiciones contractuales, en el entorno de servicios de *cloud computing*. En el marco de estos trabajos también se planteó, a raíz de la postura de la autoridad francesa de protección de datos, que pudiera considerarse la posibilidad de establecer varios modelos de cláusulas contractuales, de forma que se pudiera optar entre considerar al proveedor encargado del tratamiento o responsable conjunto[1391].

2.2. La asignación de responsabilidad a los buscadores en contra de la neutralidad y los intereses económicos alegados: el asunto *Google*

2.2.1. El contexto y la sentencia

Es imprescindible mencionar la sentencia del TJUE, de 13 de mayo de 2014, en el asunto *Google*, por su gran relevancia en algunos de los aspectos abordados en este trabajo. Esta sentencia respondió a la petición de una decisión prejudicial, por parte de la Audiencia Nacional, que debía resolver sobre un recurso interpuesto por *Google Spain, S.L.* contra una resolución dictada por el Director de la AEPD. Esta resolución obligaba a *Google* a suprimir los datos personales del denunciante, vinculados a varios anuncios relativos a una subasta de inmuebles, relacionada con un embargo, derivado de deudas a la Seguridad Social[1392]. Estos anuncios se habían publicado en un periódico (La Vanguardia), en su edición impresa en 1998 y después aparecieron también en la versión electrónica del periódico.

---

protección de datos personales de investigación 2012, Agencia Española de Protección de Datos, Agencia Estatal BOE, Madrid, 2013, págs. 60, 94 a 95.

[1391] *Liability for non-compliance with data protection obligations, rough draft presented by M-CH. ROQUES-BONET, L. NETO GALVAO, 2nd meeting of the Commission Expert Group on Cloud computing contracts, 29-30 January 2014*. http://ec.europa.eu/justice/contract/files/expert_groups/final_draft_paper_dp_liability_en.pdf (fecha consulta: 12.9.2014).

[1392] La Audiencia Nacional eligió este caso en concreto derivado de la Resolución de la AEPD 1680/2010, de 30 de julio, recaída en expediente TD/650/2010, para plantear la cuestión prejudicial ante el TJUE de entre casi un centenar de asuntos similares que afectaban a *Google*. RALLO LOMBARTE pone en duda la idoneidad de la elección de este asunto como *leading case*, ya que estima que la AEPD no debió haber eximido al periódico de la obligación de cancelar los datos en su página web. Entiende este autor que, si bien La Vanguardia podía amparar la publicación de la subasta en una obligación legal que perseguía su publicidad, tras la celebración de la misma ya no cabe esta argumentación. Al contrario de lo que sucede con los boletines oficiales que gozan de la garantía de intangibilidad de su contenido, no cabe admitir lo mismo para un anuncio administrativo que difunde un periódico. A. RALLO LOMBARTE, *El derecho al olvido en Internet, Google versus España*, Centro de Estudios Políticos y Constitucionales, Madrid, 2014, pág. 242.

El denunciante se dirigió a la editorial del periódico para solicitar la supresión de estos datos, ya que el embargo se había resuelto hacía años. La editorial se negó y manifestó que la publicación se había realizado de acuerdo con la normativa. El denunciante contactó con *Google Spain, S.L.* y le solicitó que impidiera, que, al teclear en el motor de búsqueda su nombre y apellidos, apareciera la información mencionada.

Google Spain, S.L. remitió la solicitud a *Google Inc.*, la empresa matriz ubicada en EEUU, ya que, según alegó, era esta empresa la que prestaba el servicio de búsqueda[1393]. El denunciante interpuso una reclamación ante la AEPD y solicitó a la editorial que eliminase o modificase la publicación para que no aparecieran sus datos personales. También solicitó que se exigiese a *Google* que eliminara u ocultara sus datos para que dejaran de aparecer en sus resultados de búsqueda.

Mediante resolución de 30 de julio de 2010 el Director de la AEPD estimó la reclamación contra *Google Spain, S.L.* y *Google Inc.* e instó a ambas empresas a adoptar las medidas necesarias para retirar los datos de su índice. Sin embargo, desestimó la reclamación contra la editorial porque consideró que había una justificación legal para la publicación de los datos. *Google Spain, S.L.* y *Google Inc.* interpusieron recursos ante la Audiencia Nacional y solicitaron la nulidad de la resolución de la AEPD. La Audiencia Nacional suspendió el procedimiento y planteó una cuestión prejudicial al TJUE.

La sentencia del TJUE es interesante por muchos motivos. El más conocido y evidente es que responde a la cuestión suscitada sobre el controvertido derecho al olvido[1394]. Sin embargo, el aspecto que más interesa, en el marco de este trabajo, es el análisis efectuado por el TJUE para determinar si *Google* puede ser considerado responsable del tratamiento. A continuación repasaré, mediante el método de análisis definido en este trabajo, esta calificación de *Google* como responsable del tratamiento, por parte del TJUE. Completaré la revisión de esta sentencia con la interpretación que el TJUE realiza del criterio sobre determinación de la legislación aplicable, que servirá para introducir finalmente, como ejemplo práctico de la debilidad del concepto de responsable, la aplicación por parte de la Audiencia Nacional de los dictados de la sentencia del TJUE.

[1393] Resolución 1680/2010 de la AEPD, de 30 de julio de 2010, TD/650/2010.
[1394] Ver Capítulo V.

2.2.2. El buscador como responsable del tratamiento: ¿neutralidad o responsabilidad?

a. La importancia de los buscadores en el contexto digital

Antes que nada, hay que entender la importancia que tienen los motores de búsqueda en el ecosistema digital. Los buscadores son servicios que permiten a cualquier usuario encontrar información en Internet mediante la introducción de palabras clave. Inicialmente, cuando se creó Internet, la información que se publicaba en las páginas web sólo podía encontrarse si se conocía la dirección de la página[1395]. Por tanto, la aparición de los buscadores supuso una auténtica revolución en el uso de Internet. De esta forma, el GA29 destacaba el especial papel desempeñado por estos, en el entorno digital y la necesidad de buscar un equilibrio entre el cumplimiento de la legislación de protección de datos, y el libre flujo de información y el derecho a la libertad de expresión[1396].

Lógicamente, los buscadores son gestionados por empresas que buscan un beneficio económico. Este beneficio se obtiene de la publicidad que se ofrece cuando el usuario realiza la búsqueda. Para que la publicidad sea eficaz y, por tanto, merezca la pena a los anunciantes, lo que hacen los buscadores es analizar la información que obtienen del usuario para personalizar los anuncios y adaptarlos a sus intereses[1397].

Es bastante evidente que respecto a estos datos personales, que utilizan los buscadores para proporcionar a sus usuarios publicidad personalizada, estas empresas

[1395] De hecho, se ha vuelto a ese momento previo a la existencia de los buscadores con la conocida como *deep web* o web profunda. Internet se compara con un iceberg en el que en la punta externa se encuentra la información que todos conocemos a la que se accede mediante los buscadores. En la cara interna del iceberg se encontraría información que no estaría indexada y a la que se accede mediante redes encriptadas que preservan el anonimato en la navegación como la red TOR. En este espacio oculto, además de información lícita se puede encontrar un mercado negro donde se moverían los cibercriminales. K. VÁZQUEZ, "Los bajos fondos de la red", *El País semanal Tecnología*, 14.8.2014, http://elpais.com/elpais/2014/08/13/eps/1407957234_037823.html (fecha consulta: 7.3.2015).

[1396] Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda 00737/ES WP 148, 4.4.2008, Grupo de trabajo Artículo 29 sobre la protección de datos, pág. 14.

[1397] El GA29 aludía a los buscadores como ejemplo de acumulación de datos de sus usuarios que podían llevar a completos perfiles de los mismos gracias a las búsquedas realizadas que se añadían a datos que podían identificarlos, incluso aunque se tratara de una navegación anónima (mediante las direcciones IP o la utilización de cookies u otros identificadores). El GA29 citaba el caso AOL, que en el año 2006 publicó una muestra de búsquedas y resultados de 650.000 usuarios cuyas identidades se sustituyeron por números. Sin embargo, los periodistas descubrieron que podía llegarse a identificar a estos usuarios. Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda 00737/ES WP 148, *op. cit.* págs. 4 a 5.

deben considerarse responsables del tratamiento. Sin embargo, lo que ha resultado no ser tan evidente es la calificación de responsables del tratamiento de los buscadores, respecto a la información que se origina de las páginas web a las que el buscador enlaza mediante la lista de resultados que se ofrece al usuario, en respuesta a su petición de búsqueda, mediante palabra clave. La cuestión prejudicial se circunscribió a esta actividad de los buscadores como proveedores de contenido.

Al abordar el estudio de los diferentes elementos que conforman el concepto, el elemento subjetivo, en principio, no debería plantear ninguna dificultad porque sería una sociedad, una persona jurídica (*Google Inc.*). Sin embargo, como se verá, la dificultad estribará en qué persona jurídica es la que activa el concepto, cuando le llegue la hora de aplicar la sentencia del TJUE a la Audiencia Nacional, ya que el TJUE valorará la responsabilidad del buscador en abstracto, sin concretar la persona jurídica a la que se refiere en el supuesto concreto planteado. En todo caso, en lo que atañe al análisis de los elementos del concepto serán importantes especialmente el objetivo y el funcional.

b. Elemento objetivo: existencia de tratamiento

En el caso del elemento objetivo del concepto de responsable del tratamiento, de acuerdo con lo previsto en el artículo 2.d) Directiva 95/46/CE, es "el tratamiento de datos". Una de las cuestiones que planteó la Audiencia Nacional al TJUE era si la actividad del buscador de *Google*, como proveedor de contenidos, consistente en localizar la información publicada o incluida en la red por terceros, su indexación de forma automática, el almacenamiento de la misma de forma temporal y la puesta a disposición de los internautas, con un cierto orden de preferencia, siempre que esta información contuviera datos personales, se podía considerar un tratamiento de datos, de acuerdo con lo establecido en el artículo 2.b) Directiva 95/46/CE, que define este concepto[1398].

Pese a que *Google* esgrimió como argumento que no realizaba un tratamiento de datos, el TJUE apreció que este tratamiento se llevaba a cabo, ya que las operaciones que realizaba el buscador estaban incluidas, de forma expresa, en la definición de

[1398] Sentencia del TJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2014:317, apdo 20.

tratamiento[1399]. El TJUE recordó que, el hecho de hacer referencia a datos personales en un sitio web, ya lo había considerado tratamiento anteriormente[1400].

La Audiencia Nacional, al exponer el funcionamiento del buscador, explicó que éste no intervenía en la elaboración de la información de las páginas web de terceros de las que ofrecía los enlaces ni la modificaba ni identificaba el significado de los términos que se incluían en las mismas, por lo que desconocía si eran datos personales o no[1401].

El TJUE entendió que, aunque el buscador no modificara los datos de las páginas web de origen, realizaba otras operaciones que también se consideraban tratamiento de datos, como se ha mencionado[1402]. El TJUE consideraba irrelevante que el buscador no distinguiera si los datos eran personales o no ni que estos datos hubieran sido objeto de previa publicación[1403].

[1399] El TJUE precisó en entrecomillado las operaciones que llevaba a cabo *Google* y que se incluyen en la definición de tratamiento: "al explorar Internet de manera automatizada, constante y sistemática en busca de la información que allí se publica, el gestor de un motor de búsqueda «recoge» tales datos que «extrae», «registra» y «organiza» posteriormente en el marco de sus programas de indexación, «conserva» en sus servidores y, en su caso, «comunica» y «facilita el acceso» a sus usuarios en forma de listas de resultados de sus búsquedas. Ya que estas operaciones están recogidas de forma explícita e incondicional en el artículo 2, letra b), de la Directiva 95/46, deben calificarse de «tratamiento» en el sentido de dicha disposición, sin que sea relevante que el gestor del motor de búsqueda también realice las mismas operaciones con otros tipos de información y no distinga entre éstos y los datos personales." *Ibídem*, apdo. 28.

[1400] Sentencia del TJUE de 6 de noviembre de 2003, *Bodil Lindqvist*, C-101/01, EU:C:2003:596, apdo. 25. Sentencia del TJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2014:317, apdo. 26.

[1401] Por su claridad reproduzco la explicación sobre el funcionamiento de los buscadores de la Audiencia Nacional: "La actividad de los buscadores, como proveedores de contenidos, podría sintetizarse como sigue: Dada la gran cantidad de información disponible en Internet los buscadores permiten a los usuarios acceder a la misma de forma rápida, introduciendo criterios de búsqueda (palabras, grupos de palabras o simplemente caracteres). Los buscadores, con la finalidad de facilitar y acelerar la búsqueda, rastrean previamente los servidores de contenidos conectados a la red mediante un software (conocidos como robots o arañas) para que les proporcionen información sobre los contenidos existentes en los mismos. Con esta información elaboran un índice de palabras (con millones de palabras) que relacionan con la referencia a las páginas web en la que aparece esa palabra. Esta información se almacena y periódicamente se actualiza visitando las páginas de origen conforme a las instrucciones recibidas por la empresa que gestiona el buscador. Los buscadores no intervienen en la elaboración de dicha información, ni la modifican, ni identifican el significado de los términos (desconociendo si se trata de una palabra sin sentido alguno, del nombre de una persona o de cualquier otro significado). El buscador como respuesta a la solicitud de información del usuario muestra una pantalla con un listado de direcciones web asociadas las palabras claves proporcionadas, permitiendo que el usuario acceda directamente al contenido del servidor web que aloja dicha información seleccionando el enlace que le facilita el buscador. El resultado de la búsqueda es ordenado por unos criterios de preferencia que establece el buscador." AAN de 27 de febrero de 2012 (Sala de lo contencioso-administrativo) (ROJ: AAN 19A/2012), FJ 4.

[1402] Sentencia del TJUE de 6 de noviembre de 2003, *Bodil Lindqvist*, C-101/01, EU:C:2003:596, apdo. 31.

[1403] Como había indicado el tribunal en una sentencia anterior, el hecho de que los datos tratados ya hubieran sido objeto de publicación previa en medios de comunicación, no permitía que se excepcionara la aplicación de la Directiva 95/46/CE, ya que entender lo contrario supondría vaciar de contenido a la directiva. Sentencia del TJUE de 16 de diciembre de 2008, *Tietosuojavaltuutettu/Satakunnan*

Esta valoración que realizó el TJUE respondía a los argumentos que el Abogado General Niilo Jääskinen (en la línea de lo indicado por la Audiencia Nacional en su auto) esgrimió, en virtud de este automatismo y la no alteración de la información por parte del buscador para entender que no podía ser calificado de responsable del tratamiento. Esta argumentación derivaba de la consideración del especial papel de intermediario atribuido al buscador. No obstante, con el fin de seguir los pasos establecidos en el análisis del concepto de responsable, hay que ubicar estos argumentos del Abogado General en el estudio del elemento funcional, es decir, en el análisis de si el buscador determinaba los fines y los medios del tratamiento[1404].

c. Elemento funcional: adaptación de la norma al contexto, el debate sobre el factor de la consciencia y la neutralidad del servicio

i. La comparación con el caso Lindqvist para realizar una interpretación amplia de la Directiva 95/46/CE

El Abogado General, en sus conclusiones, propugnaba realizar una interpretación de la Directiva 95/46/CE para adaptarla a un contexto que no existía en el momento de su aprobación y que, por tanto, el legislador no pudo tener en cuenta[1405]. El Abogado General realizó un justificado paralelismo entre este asunto sobre el derecho al olvido y el asunto *Lindqvist*, ya que en éste último también se puso en entredicho el funcionamiento de Internet.

En el asunto *Lindqvist*, se argumentó que el estado de desarrollo de Internet, cuando se aprobó la Directiva 95/46/CE, había impedido que el legislador tuviera en mente incluir la publicación de datos en un sitio web, en el concepto de transferencia internacional de datos. Por ello, el tribunal, en el mencionado asunto, lo que hizo fue

---

Markkinapörssi Oy, Satamedia Oy, C-73/07, EU:C:2008:727, apdos. 48 y 49. Sentencia del TJUE de 6 de noviembre de 2003, *Bodil Lindqvist*, C-101/01, EU:C:2003:596, apdo. 30.

[1404] El Abogado General consideraba que las operaciones que realizaba *Google* debían considerarse tratamiento de datos y que la cuestión clave radicaba en si se debía considerar a *Google* responsable del tratamiento respecto a este tratamiento. Conclusiones del Abogado General Niilo Jääskinen de 25 de junio de 2013 en el asunto *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2013:424, apdo. 72.

[1405] *Ibídem*, apdos 77, 78.

adoptar una interpretación que no bloqueara el uso de Internet y consideró que no debía calificarse de transferencia internacional la difusión de datos a través de su publicación en sitios web. Si se hubiera aplicado de forma literal la Directiva 95/46/CE y se hubiera encajado esta publicación en el concepto de transferencia, hubiera tenido unas implicaciones muy importantes en el uso de Internet[1406].

No obstante, la interpretación del Abogado General lo que perseguía claramente era anteponer el funcionamiento del buscador a la protección del derecho[1407]. No puede equipararse, el alcance interpretativo de la sentencia *Lindqvist* con el que reclamaba el Abogado General en este asunto. En la sentencia *Lindqvist* se optó por entender que no se podía aplicar la regulación de las transferencias internacionales de datos a la publicación de datos, una regulación especial que, si bien, forma parte del marco legal del derecho a la protección de datos, sólo es uno de los aspectos que cubre. En el presente caso analizado, el Abogado General pretende eludir la aplicación del régimen general del derecho.

Con el fin de realizar una interpretación de la Directiva 95/46/CE, que tuviera en cuenta la evolución tecnológica y, más concretamente, la existencia de los buscadores, el Abogado General entendió que había que acudir al principio de proporcionalidad, a los objetivos de la Directiva y a los medios que ésta proporciona para su cumplimiento, con el fin de hallar un resultado equilibrado y razonable[1408]. En consecuencia, alegó que para

[1406] Además esto se hubiera añadido a la otra interpretación que se realizó mediante esta sentencia. El TJUE entendió que la difusión en Internet de datos personales a un grupo indeterminado de personas, aunque fuera realizada por un particular en el ejercicio de actividades que podían en principio considerarse dentro de la excepción del uso personal y doméstico, no podía ser incluida en esta excepción. Por tanto, si se hubieran sumado estos dos aspectos se hubiera dificultado sobremanera el uso de Internet. Sentencia del TJUE de 6 de noviembre de 2003, *Bodil Lindqvist*, C-101/01, EU:C:2003:596, apdo. 47.

[1407] Ello se ilustra con la afirmación que realizó el mismo Abogado respecto a que, si se siguiera una interpretación literal e incluso teleológica de la Directiva 95/46/CE, se afirmaría la responsabilidad del buscador, como sugerían todas las partes del litigio (excepto *Google* y el Gobierno helénico). Conclusiones del Abogado General Niilo Jääskinen de 25 de junio de 2013 en el asunto *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2013:424, apdo. 77.

[1408] *Ibídem*, apdo. 79. RALLO LOMBARTE es muy crítico con el enfoque del Abogado General que acude al principio de proporcionalidad, con el fin de defender una aplicación moderada y "evitar consecuencias jurídicas poco razonables y excesivas" (Conclusiones del abogado general Niilo Jääskinen en el asunto C-131/12, apdo. 30) y, sin embargo, según el autor, este principio se aplica "transgrediendo el ejercicio interpretativo derivado de la aplicación del principio de proporcionalidad que obliga a enjuiciar la posibilidad de conciliar los derechos e intereses en juego evaluando si los fines pretendidos podían alcanzarse con medios ajustados a los mismos". De esta forma, lo que hace el Abogado General, según el autor, es anteponer los intereses económicos de los operadores por encima del derecho fundamental a la

que se activara el rol de responsable del tratamiento, éste debía tratar los datos con una intención que se relacionara con su tratamiento como datos personales. De esta forma, el Abogado General estimó que del contenido de las disposiciones materiales de la Directiva 95/46/CE (arts. 6, 7 y 8), se deducía que el responsable debía saber lo que hacía respecto a los datos que trata, debía ser consciente de los datos que trataba y del por qué los trataba. La información que trataba el responsable debía ser semánticamente relevante para él y no un mero código informático[1409].

ii. El factor de la consciencia esgrimido por el Abogado General

El Abogado General estableció, por tanto, como principal argumento para considerar que el buscador no era responsable del tratamiento, el hecho de su inconsciencia al tratar datos personales, del automatismo del tratamiento[1410]. Sin embargo, afirmó, al mismo tiempo, que hay supuestos en los que el buscador sí deberá considerarse responsable. Estos supuestos los limitó a cuando el buscador decidiera no respetar los códigos de exclusión establecidos por el titular de la página web origen de la información y cuando no actualizara alguna página web de su memoria oculta (*cache*), cuando ello fuera solicitado por el titular de la página web origen. Por tanto, hay que entender que, en estos supuestos, el Abogado General consideró que *Google* era consciente de los datos. Sin embargo, no se aprecia diferencia en la utilización del automatismo del servicio que tampoco, en estos casos en los que el Abogado General considera que *Google* es responsable, será consciente de que los datos son personales[1411].

En realidad, lo que hizo el Abogado General es apoyarse en el enfoque adoptado por el GA29 en su dictamen sobre los buscadores, pero sin acogerlo plenamente[1412]. El GA29 también había esgrimido el principio de proporcionalidad para entender que, cuando el buscador actuaba como proveedor de contenidos, como servicio de

protección de datos. A. RALLO LOMBARTE, *El derecho al olvido en Internet, Google versus España*, *op.cit.*, pág. 257.

[1409] Conclusiones del Abogado General Niilo Jääskinen de 25 de junio de 2013 en el asunto *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2013:424, apdo. 83.

[1410] *Ibídem*, apdo. 84.

[1411] Lo mismo considera A. RALLO LOMBARTE, *El derecho al olvido en Internet, Google versus España*, *op.cit.*, págs. 263 a 264.

[1412] Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda, *op. cit.* págs. 14 a 16.

intermediación, no debía ser considerado responsable principal, sino que este papel debía reservarse a las páginas de origen de la información[1413]. Sin embargo, el GA29 no excluyó la responsabilidad total del buscador sino que, en virtud de su papel específico de intermediario, lo que entendió es que su responsabilidad ante el tratamiento de datos estaba limitada a la posibilidad de eliminar los datos de su índice y de los resultados[1414].

Para establecer los supuestos en los que el buscador debía proceder a esta eliminación de datos, el GA29 remitía a la legislación nacional reguladora de la responsabilidad[1415]. Por tanto, el GA29 no sólo limitaba la responsabilidad sino que además remitía a otras normas para determinarla. El GA29 especificaba que en algunos Estados miembros se había regulado de forma específica la responsabilidad de los buscadores de eliminar los datos en virtud del derecho de oposición del artículo 14 de la Directiva 95/46/CE y de la Directiva 2000/31/CE[1416].

También el Abogado General se refirió a las exclusiones de responsabilidad para los servicios de intermediación de la sociedad de la información de la Directiva 2000/31/CE (arts. 12 a 14) y, además, añadió el Considerando 47 Directiva 95/46/CE como argumentos para excluir la responsabilidad del buscador[1417].

[1413] *Ibídem.*

[1414] De hecho, el GA29 parecería que apuntaba a un supuesto de corresponsabilidad en el que, tanto el buscador, como los editores de las páginas de origen, se responsabilizaban de la información referida a estas páginas reflejadas en los resultados. En ese caso, podría argumentarse que, en algunos casos los editores de los sitios web, además de la finalidad que persigan al publicar la información, persiguen también la finalidad de que esta información publicada pueda ser hallada por los usuarios de los buscadores. En este sentido, si no excluyen la indexación es que persiguen esa finalidad y, por tanto, ambos, buscador y editores perseguirían un mismo fin. *Ibídem*, pág. 15.

[1415] El GA29 se refiere a la "*general tort law and liability regulations of the particular Member State*" que en la versión española se traduce como "derecho delictual general y de las disposiciones sobre responsabilidad del Estado miembro concreta". *Ibídem.*

[1416] Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda, *op. cit.*, pág. 15, Nota al pie 18.

[1417] Hay que matizar que la sentencia en español indica "Sobre este punto me gustaría distanciarme del principio contenido en el considerando 47 de la Directiva". Sin embargo entiendo que no sería una traducción adecuada de la sentencia en versión original, inglesa que indica: "*Here I would draw from the principle expressed in recital 47 in the preamble to the Directive"*. Por tanto, interpreto que el Abogado General lo que quería era apoyar sus argumentos con el considerando y no distanciarse del mismo. Conclusiones del Abogado General Niilo Jääskinen de 25 de junio de 2013 en el asunto *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2013:424, apdo. 87.

Así, el Considerando 47 Directiva 95/46/CE se refiere a los servicios de telecomunicaciones o correo electrónico cuyo objeto es transmitir mensajes[1418]. En este caso, este Considerando 47, claramente, no se podría aplicar a los buscadores cuyo objetivo no es la mera transmisión de mensajes[1419]. La Directiva 2000/31/CE se refiere a los prestadores de servicios de la sociedad de la información que se califican como intermediarios que son: los servicios de alojamiento, los de *caching* y los de transmisión o acceso a Internet.

Como se puede ver, tanto el Considerando 47, como las exclusiones de responsabilidad de la Directiva 2000/31/CE atribuyen un régimen específico para una tipología de prestadores a los que se ha otorgado, en el nuevo contexto tecnológico, un papel preponderante.

Pese a no incluir en este catálogo los servicios de motor de búsqueda, se planteó al TJUE si podía aplicarse esta regulación al servicio de referenciación de *Google* (el servicio *Adwords*), es decir el servicio de venta de publicidad[1420]. Este servicio permite a las empresas seleccionar una o varias palabras clave para que, en el caso de que coincidan con las que un internauta introduzca en el motor de búsqueda de *Google*, se muestre el enlace promocional de esta empresa. Este enlace promocional aparece bajo la rúbrica "enlaces patrocinados" y se acompaña de un breve mensaje comercial.

El TJUE entendió que podría aplicarse la exclusión de responsabilidad relativa a servicios de alojamiento (art. 14 Directiva 2000/31/CE), ya que *Google* almacenaba un contenido que le proporcionaba la empresa anunciante[1421]. Para ello, los tribunales nacionales deberían valorar si *Google* cumplía con el carácter de "prestador intermediario", que exigía la Directiva 2000/31/CE. Es decir, su actividad debería tener

[1418] Ver Capítulo II.

[1419] El GA29 estima que los servicios de buscador quedarían fuera del ámbito de aplicación de la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas, ya que considera que son servicios que ejercen control editorial sobre el contenido, excepto en lo que se refiere a la aplicación de las previsiones de esta directiva que se aplican a todo tipo de servicios (art. 5 sobre *cookies* y art. 13 sobre comunicaciones comerciales). Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda, *op.cit.*, págs. 12 y 13.

[1420] Sentencia del TJUE de 23 de marzo de 2010, *Google France SARL y Google Inc./Louis Vuitton Malletier SA y otros*, C-236/08 a C-238/08, EU:C:2010:159.

[1421] Este precepto permite la exclusión de responsabilidad a "un servicio de la sociedad de la informaciónn consistente en almacenar datos facilitados por el destinatario del servicio", de forma que no podrá ser considerado responsable de estos datos, a menos que, tras llegar a su conocimiento la ilicitud de los mismos, no actúe con prontitud para retirar los datos o hacer evitar el acceso a los mismos.

una naturaleza "meramente técnica, automática y pasiva", lo que implicaría que el prestador "no tiene conocimiento ni control de la información transmitida o almacenada"[1422].

A esto hay que añadir que, en algunas legislaciones nacionales, como la española, al transponer las exclusiones de la Directiva 2000/31/CE, se incluyó también a los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda (art. 17 LSSI). Estos prestadores no serán responsables de la información a la que enlacen siempre que no tengan conocimiento efectivo de que esta información es ilícita o lesiona bienes o derechos de un tercero o, si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace.

El GA29, entiendo que en línea con la jurisprudencia mencionada del TJUE, indicó que, si el buscador se dirigía activamente a la información a la que enlazaba, de forma que reconociera los datos personales, ya no actuaba como intermediario y, en esos casos, debía ser calificado de responsable del tratamiento. En caso contrario, el GA29 estimaba que el buscador actuaba como un intermediario cuando "la búsqueda, el análisis y la indexación pueden realizarse de forma automática sin revelar la presencia de información personalmente identificable"[1423]. Aquí es donde hallamos el origen del argumento de la inconsciencia. La Audiencia Nacional, al exponer el funcionamiento del

[1422] Considerando 42 Directiva 2000/31/CE. El TJUE consideró que, respecto al servicio de referenciación de *Google*, para poder llegar a valorar si realmente esta empresa cumplía con los requisitos indicados, debía tenerse en cuenta el papel que desempeña *Google* en la redacción del mensaje comercial que acompaña al enlace promocional o en el establecimiento o la selección de palabras clave. Estos elementos son los que debía tener en cuenta el tribunal nacional para determinar si *Google* tenía un papel activo o no, que pudiera darle conocimiento o control de los datos almacenados y, por tanto, no permitiera la aplicación de la exención. Sentencia del TJUE de 23 de marzo de 2010, *Google France SARL y Google Inc./Louis Vuitton Malletier SA y otros*, C-236/08 a C-238/08, EU:C:2010:159, apdos. 112, 113, 118. En referencia al operador de un mercado electrónico, *e-Bay*, el TJUE también se refirió al artículo 14 Directiva 2000/31/CE, para entender que se aplicaría esta exención de responsabilidad si el operador no desempeña un papel activo que le permita adquirir conocimiento o control de los datos almacenados. Este papel lo desempeña el operador cuando presta una asistencia consistente en optimizar la presentación de las ofertas de venta y en promover estas ofertas. Sentencia del TJUE de 22 de septiembre de 2011, *Interflora Inc* y *Interflora British Unit/ Mark&Spencer plc* y *Flowers Direct Online Ltd,* C-323/09, EU:C:2011:604, apdo. 116.

[1423] El GA29 alude a que existen tecnologías sofisticadas que emplean los buscadores, cada vez más, para realizar las búsquedas, como el reconocimiento facial, por lo que no queda claro hasta qué punto esto se consideraría un comportamiento pasivo. Así, entiende el GA29 que si el buscador llevara a cabo operaciones de valor añadido relacionadas con las características de los datos que procesa se le tendría que considerar responsable del tratamiento. En caso de que además utilizara la memoria *caché* para almacenar la información, si prolongase este almacenamiento más allá de lo necesario, también consideró que desencadenaría la responsabilidad del buscador o si no respetara los códigos de autoexclusión de las páginas web de origen de la información. Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda, *op. cit.*, pág. 15.

buscador recogió esta argumentación sobre el desconocimiento del buscador, al tratar los datos[1424], y después el Abogado General acogió también esta tesis e indicó que estas disposiciones (el Considerando 47 y las exclusiones de la Directiva 2000/31/CE) respondían a que estos prestadores establecen una relación automática, técnica y pasiva con el contenido almacenado o transmitido[1425].

De hecho, la AEPD, en la resolución recurrida que da pie después al planteamiento de la cuestión prejudicial, también acudió a la regulación de la LSSI. De esta forma, pretendía reforzar la determinación de la ley aplicable mediante la alusión a la LSSI, ya que ésta dispone su aplicación a los prestadores que estén establecidos en países que no sean miembros de la UE o del EEE y dirijan sus servicios al territorio español[1426].

Así, la AEPD preparaba otra posible vía para aplicar la legislación de protección de datos en aras a que no se considerara aplicable la LOPD a *Google* por los otros criterios esgrimidos. Por tanto, la AEPD utilizó los preceptos de la LSSI para asegurar la aplicación de la regulación de protección de datos, ya que la resolución se centraba básicamente en la determinación de la legislación aplicable. No se utilizó esta normativa para argumentar que *Google* era responsable del tratamiento.

[1424] AAN de 27 de febrero de 2012 (Sala de lo contencioso-administrativo) (ROJ: AAN 19A/2012), FJ 4.
[1425] Conclusiones del Abogado General Niilo Jääskinen de 25 de junio de 2013 en el asunto *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2013:424, apdo. 87.
[1426] La AEPD acudía al artículo 8 LSSI, que se aplica a todos los servicios de la sociedad de la información que están dentro del ámbito de aplicación de la ley, y que dispone que si estos servicios atentan contra los principios enunciados, los órganos competentes para su protección podrán adoptar las medidas necesarias para que se interrumpa su prestación o se retiren los datos que los vulneren. Entre estos principios se encuentra el del respeto a la dignidad de la persona que la AEPD enlazó con la sentencia del Tribunal Constitucional STC 292/2000 que estableció el derecho a la protección de datos como una garantía que se extiende a la esfera de los bienes de la personalidad que van unidos a este respeto de la dignidad personal. Así, la afectación del derecho de protección de datos puede atentar contra el principio de respeto de la dignidad de la persona. Además la AEPD consideró aplicable el artículo 17 LSSI que es el que establece la exclusión de responsabilidad para los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda. La exclusión se aplica si estos prestadores no tienen lo que se denomina conocimiento efectivo de que la actividad o la información a la que remiten es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización o si tienen ese conocimiento actúan con diligencia para suprimir o inutilizar el enlace. El conocimiento efectivo existe cuando un órgano competente ha declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos o se hubiera declarado la existencia de la lesión y el prestador conociera la resolución, sin perjuicio de otros medios de conocimiento que pudieran establecerse. La AEPD, por tanto, en aplicación de estos artículos argumentó que podía requerir a *Google* para que adoptara las medidas necesarias para estimar la solicitud de reclamante y retirar los datos de su índice.

Acoger este argumento relativo a la consciencia entrañaría graves consecuencias para otros entornos, como puede ser el mencionado fenómeno del *big data,* ya que, en la medida en que el tratamiento de datos se considerara que se hace de forma "inconsciente", se evitaría la aplicación de la normativa de protección de datos. Hay que traer a colación lo indicado acerca del uso de los algoritmos o el proceso de hacer anónimos los datos.

El uso de algoritmos no puede considerarse un uso inconsciente de los datos, ya que tras la programación del algoritmo esta la capacidad de decisión de un responsable. No puede equipararse el tratamiento de datos, que supone el uso de un algoritmo, al tratamiento de datos que realiza un operador de telecomunicaciones cuando transmite datos a través de los canales de comunicación y donde sí se establece una relación automática, técnica y pasiva respecto al contenido transmitido. Google utiliza un algoritmo para decidir el orden en el que salen los enlaces en la lista de resultados que le aparece al usuario. Por lo que, al establecer que el tratamiento realizado por Google era inconsciente, significaría que el uso de algoritmos puede calificarse de inconsciente también.

La inconsciencia también la podemos comparar con el uso del anonimato. Si en el anonimato indicábamos que hay que tener en cuenta el riesgo de la posible reversión, en función del progreso tecnológico, con el factor de la inconsciencia hay que tener presente que se puede tornar en consciencia, sin más limitación que la voluntad del sujeto que trata los datos. Por otro lado, es mucho suponer el hecho de considerar que el legislador actual hubiera querido que en el concepto de tratamiento de datos automatizado se hubiera tenido en cuenta que debía incorporar este requisito de la consciencia.

No obstante, lo que se podría haber hecho es alegar las disposiciones mencionadas como posibles argumentos para debatir si se podía activar el elemento funcional del responsable[1427]. Es decir, el Considerando 47 Directiva 95/46/CE y las exclusiones de responsabilidad podían ser indicios de que *Google* no tenía capacidad de determinar los

[1427] RALLO LOMBARTE entiende que el Abogado General al aplicar el principio de proporcionalidad lo que hace es anteponer "elementos valorativos dignos de protección pero de valor jurídico netamente diferenciado (los objetivos de la sociedad de la información y los intereses de los operadores económicos por encima del derecho fundamental a la protección de datos)". A. RALLO LOMBARTE, *El derecho al olvido en Internet, Google versus España*, *op.cit.*, pág. 257.

fines y los medios de los datos controvertidos referidos a las páginas web de terceros. Eran argumentos legales que apuntaban a que este tipo de servicios de intermediación tenían un especial papel que se les propociona en función de su neutralidad y su utilidad. No obstante, entiendo que no existía esta neutralidad.

De todas formas, tampoco parece que las exclusiones de responsabilidad, en concreto, pudieran considerarse un argumento sólido, ya que, en todo caso lo que hacen es excluir responsabilidad, no atribuirla. La atribución debe buscarse en otras leyes, como puede ser la de protección de datos a la que, por ejemplo remite específicamente la LSSI (art. 1.2 LSSI).

iii. El TJUE atribuye la responsabilidad al buscador precisamente por su rol específico

El TJUE simplificó la conclusión, al considerar el tratamiento en global, es decir, sin hacer distinción entre la parte referida a las páginas web de origen y a lo que se refería puramente al índice de resultados. El tribunal consideró que el tratamiento sobre el que el buscador era responsable eran todas las operaciones que le llevaban a prestar el servicio y que integraban los datos personales que podían contenerse en las páginas web de origen.

De forma contundente, el TJUE señaló que sería contrario al tenor del concepto de responsable del tratamiento y a su objetivo de garantizar una protección eficaz y completa de los interesados, mediante una definición amplia, excluir del mismo al buscador debido a que no ejerce un control sobre los datos personales, publicados en las páginas web de terceros[1428]. A continuación, el TJUE aclaró en la sentencia, que el tratamiento que lleva a cabo el buscador se diferencia del que efectúan los terceros editores de las páginas web a las que enlaza, que lo que hacen es publicar los datos. Este tratamiento diferenciado que realiza el buscador se añade al de estos editores[1429].

En respuesta a que los editores de los sitios web tienen la facultad de evitar la indexación, por parte de *Google* mediante los códigos de exclusión, el TJUE indicó que

[1428] Sentencia del TJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2014:317, apdo. 34.
[1429] *Ibídem*, apdo. 35.

ello no implica la liberación de responsabilidad de los buscadores[1430]. En este caso, el TJUE apuntó a un posible caso de corresponsabilidad, en el que tanto los editores de los sitios web, como el buscador serían responsables[1431].

En contraste con la postura del Abogado General, que lo que pretendía era la exclusión de responsabilidad del buscador por su papel de intermediario, el TJUE lo que hizo fue incidir en ese rol, pero con el fin de atribuirle la responsabilidad. Para el tribunal europeo la actividad del buscador afecta significativamente y de modo adicional a la que desarrollan los editores de las páginas web, a los derechos fundamentales de respeto de la vida privada y de protección de datos personales[1432]. Por tanto, al determinar los fines y los medios de esta actividad, debe garantizar el cumplimiento de la Directiva 95/46/CE.

Pese a esta contundencia, el TJUE parece abrir un poco la puerta a una posible modulación de la responsabilidad, al indicar que el buscador debe garantizar "en el marco de sus responsabilidades, de sus competencias y de sus posibilidades" que la actividad de motor de búsqueda satisface las exigencias de la Directiva 95/46/CE[1433].

Esto también plantea las posibles consecuencias relativas al cumplimiento del estatuto del responsable por parte de *Google*. El Abogado General también aludió a la imposibilidad del buscador de cumplir con sus obligaciones para rechazar la responsabilidad del buscador[1434]. El GA29 ya recalcó que no se podía utilizar esta imposibilidad de cumplimiento como argumento para excluir la activación de la responsabilidad[1435]. Sin embargo, desde un punto de vista práctico, ¿qué implicaciones tendrá esta imposibilidad?

[1430] *Ibídem*, apdo. 39.
[1431] *Ibídem*, apdo. 40.
[1432] *Ibídem*, apdo. 38.
[1433] *Ibídem*.
[1434] El Abogado General estima que el buscador no puede ni jurídicamente ni de hecho cumplir las obligaciones del responsable del tratamiento establecidas en los artículos 6,7 y 8 Directiva 95/46/CE respecto a los datos personales contenidos en páginas web fuente alojadas en servidores de terceros. Conclusiones del Abogado General Niilo Jääskinen de 25 de junio de 2013 en el asunto *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2013:424, apdos. 89, 90.
[1435] El GA29 mencionó que, especialmente en casos de corresponsabilidad el hecho de no estar en condiciones de cumplir directamente todas las obligaciones que incumben al responsable del tratamiento no excluye que se sea responsable del tratamiento. Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.*, pág. 24.

Si seguimos la interpretación estricta de la Directiva 95/46/CE, *Google*, por ejemplo, debería informar a las personas, cuyos datos trate. El buscador debería dirigirse a las personas, cuyos datos se hallen en las páginas web de origen, para cumplir con este deber de información. Parece evidente que todos aquellos que utilizan Internet conocen que los datos son tratados por los buscadores. Sin embargo, con el marco legal vigente esta razón no puede ser esgrimida por el buscador. Lo único que le quedaría es acogerse a la previsión contenida en el artículo 11.2 Directiva 95/46/CE, que permite que no se aplique la obligación de informar, cuando ésta resulte imposible o exija esfuerzos desproporcionados. Sin embargo, en este caso habrá que acudir a las leyes nacionales, ya que esta misma disposición indica que los Estados miembros establecerán las garantías apropiadas[1436].

También esto debe enlazarse con la responsabilidad de los titulares de las páginas web de origen de los datos, que realizan estrictamente una comunicación de datos a *Google*. Por tanto, estos titulares deberán valorar la legitimación de esta comunicación. Sin duda, esta sentencia refuerza las garantías de protección, aunque resta ver las posibles consecuencias reales de la misma.

Este pronunciamiento es importante respecto a la configuración del responsable en el contexto digital, ya que supone el rechazo del argumento de la neutralidad y el automatismo del tratamiento. La relevancia del responsable queda patente en el hecho de que la activación de la responsabilidad será requisito previo para poder aplicar la normativa. Es decir, si ante los razonamientos del Abogado General, el TJUE hubiera aceptado que *Google* no era responsable del tratamiento, ya no hubiera tenido que analizar ningún aspecto adicional. Debe reafirmarse, por tanto, el papel clave de esta figura.

iv. La superación de la interpretación del primer criterio del artículo 4 Directiva 95/46/CE sobre la legislación aplicable en los asuntos contra Google

[1436] A modo de ejemplo, en el caso español, la LOPD establece en su artículo 5.5 la necesidad de que el responsable que quiera acogerse a esta posibilidad debe solicitar autorización a la AEPD en un procedimiento específico.

Aunque se haya deducido, en función del análisis de los elementos, que el sujeto es un responsable del tratamiento, habrá que ver si supera la aplicación de los criterios que, en el ámbito territorial, originan la aplicación de la legislación.

En este sentido, se puede retomar el análisis realizado anteriormente relativo a los criterios que determinan en la Directiva 95/46/CE la legislación aplicable[1437]. Hay que recordar que se planteaba la relación entre la activación del papel de responsable con la aplicación del primer criterio, que exigía que el tratamiento se llevara a cabo en el marco de las actividades de un establecimiento del responsable del tratamiento ubicado en territorio de un Estado miembro. Concretamente se aludía al supuesto en el que un responsable podía tener varios establecimientos en el territorio europeo y cómo se podía arreglar el conflicto de leyes en estos casos.

En la sentencia del TJUE sobre *Google* se aborda la cuestión de la legislación aplicable en el contexto de Internet y específicamente respecto a este buscador[1438]. Sin embargo, en este caso, se centra el debate en la matriz estadounidense (*Google Inc.*) y su filial española (*Google Spain, S.L.*).

Es importante tener en cuenta que cuando el TJUE analiza la cuestión sobre si *Google* es responsable del tratamiento, no se refiere a *Google* en concreto sino que lo que hace es aludir a un gestor de un motor de búsquedas. Por tanto, no aclara si al hacer mención de este gestor se refiere concretamente a *Google Inc.* o a *Google Spain, S.L.* o a ambas sociedades. Es lógico que el TJUE plantee la respuesta de una forma neutra, ya que es una interpretación que podrá extenderse a otros buscadores y son los tribunales nacionales los que deben aplicar esta interpretación de la Directiva 95/46/CE a los casos concretos que se les planteen.

El TJUE establece en la sentencia, entre otros, como un hecho, que el órgano remitente, la Audiencia Nacional, considera acreditado, el que *Google Inc.*, empresa matriz del grupo *Google*, con domicilio en Estados Unidos, es la que gestiona *Google*

[1437] Ver Capítulo IV.
[1438] Sentencia del TJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2014:317.

Search, el buscador de *Google*[1439]. Por tanto, se puede entender que, al calificar a un gestor de un motor de búsqueda como responsable del tratamiento, en el concreto caso del grupo de empresas de *Google*, ese gestor del motor de búsquedas será *Google Inc.*, si bien es la Audiencia Nacional quien, en definitiva debe realizar, como veremos, esa calificación.

Para poder aplicar la Directiva 95/46/CE, es necesario que se pueda activar alguno de los criterios del artículo 4 Directiva 95/46/CE. El primero de estos criterios, como se ha mencionado, establece que el tratamiento se efectúe en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio de un Estado miembro (art. 4.1.a) Directiva 95/46/CE).

Pues bien, *Google* argumentaba que no podía utilizarse este criterio ya que, la filial española, *Google Spain, S.L.*, no intervenía de ninguna forma en el tratamiento de datos del buscador, una actividad que gestionaba la matriz[1440]. *Google Spain, S.L.* llevaba a cabo la actividad publicitaria en España. El gobierno español y la Comisión Europea defendían que el criterio del artículo 4.1.a) Directiva 95/46/CE no exigía que el tratamiento fuera realizado "por" el propio establecimiento, sino que lo que requería era que se realizara "en el marco de las actividades" de éste[1441].

El TJUE optó en la sentencia por una interpretación amplia del criterio y lo justificó con la intención del legislador, a la que atribuyó el deseo de que no se excluyera la protección que brindaba la directiva[1442]. Por tanto, el tribunal consideró que el hecho de que *Google Inc.* tuviera una filial en España que gestionaba la venta de publicidad que sirve para rentabilizar el servicio del buscador, era suficiente para aplicar este criterio, al entender que existía un tratamiento que se realizaba, en el marco de las actividades del establecimiento del responsable[1443].

Con esta interpretación algo forzada del tribunal europeo destinada a una aplicación territorial amplia, se resuelven las dudas que sugería en mi análisis del criterio

[1439] *Ibídem*, apdo. 43.
[1440] Sentencia del TJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2014:317, apdo. 51.
[1441] *Ibídem*, apdo. 52.
[1442] *Ibídem*, apdo. 54.
[1443] *Ibídem*, apdo. 55 a 57.

del artículo 4.1.a) Directiva 95/46/CE. En este caso, tenemos a la matriz estadounidense, que es la responsable del tratamiento, ya que es la que determina los fines y medios del tratamiento relacionado con el buscador. Por tanto, la filial española no activaría los criterios para poder ser considerada responsable del tratamiento ni tampoco puede ser considerada encargada del tratamiento. Así, se amplía la interpretación de lo que se considera realizar el tratamiento, en el marco de las actividades del establecimiento, de forma que parece que, en conclusión, basta con que el responsable tenga un establecimiento en suelo europeo y que su actividad esté ligada, de alguna forma, al negocio de buscador.

Sin embargo, esta interpretación se podría considerar que es la que saca más utilidad a este criterio, que, como se apuntaba en el estudio, si se ligara a la activación de algún rol de responsable o de encargado no sería, al final, tan práctico.

También la AEPD desligó la aplicación del punto de conexión a la activación de la responsabilidad. Así, en la resolución que dictó contra *Google*, que originó la cuestión prejudicial, precisamente estimó que el hecho de aplicar, como punto de conexión, que *Google Spain, S.L.* es un establecimiento que el responsable tiene en territorio español, no afectaba a la atribución de responsabilidad[1444].

La AEPD consideró que, a quien debía imputarse la responsabilidad, era a *Google Inc*, ya que era quien llevaba a cabo las operaciones de tratamiento y quien reconocía, que respondía, de forma automática, por las sanciones que pudieran imponerse a *Google Spain, S.L.*. La AEPD hacía referencia, principalmente, a que, en virtud de lo alegado por *Google*, la filial española se identificaba subjetivamente con la matriz y que ésta última respondía de las actividades que llevaba a cabo ella misma y la filial. Sorprendentemente, la AEPD no mencionaba que la matriz era la que determinaba los fines y los medios, como argumento para responsabilizarla[1445].

Sin embargo, bastaría que *Google Inc.* cerrara todas las empresas que tiene en el territorio europeo, para evitar la aplicación de este primer criterio. Quedaría, por tanto, como último recurso, la aplicación del tercer criterio, establecido en el art. 4.1.c)

[1444] Resolución R/02892/2013 de 18 de diciembre de 2013, PS/00345/2013, FJ XVIII.
[1445] *Ibídem.*

Directiva 95/46/CE, criterio que no ha interpretado el TJUE, en la sentencia referenciada, al haber determinado la aplicación del primero.

En cambio, la AEPD no se limitó a considerar aplicable el criterio relativo al establecimiento, sino que afirmó que se podría aplicar el criterio de la LOPD que se refiere a la utilización por parte de un responsable del tratamiento, establecido en un país fuera del EEE, de medios en el territorio español. Y ello porque la AEPD entiende que la instalación de *cookies* en el ordenador de un usuario, ubicado en territorio español, debe entenderse como un recurso a medios en este territorio[1446].

Claramente se puede concluir de estas apreciaciones que los criterios sobre legislación aplicable establecidos en la Directiva 95/46/CE se han forzado para poder asegurar la máxima protección de los derechos de los afectados, en el entorno digital[1447]. Era necesario revisar los criterios de aplicación de la normativa y ha sido uno de los aspectos que más claramente se ha introducido en el proyecto de reforma de la Directiva 95/46/CE.

v. Un ejemplo de la fragilidad del concepto: la aplicación por la Audiencia Nacional de la sentencia del TJUE sobre Google

Sin embargo, aún nos falta otra pieza más de este puzle, que ha sido este asunto *Google,* tan importante para el derecho de protección de datos. Esta pieza era la aplicación de la sentencia en el derecho español mediante la resolución de los más de

[1446] *Google* admitió en el procedimiento utilizar centros de datos que estaban ubicados en el EEE pero negaba que estuvieran en España. Además rechazaba que se pudieran entender como medios los equipos pertenecientes a los usuarios, ya que interpretaba que la expresión "utilice en el tratamiento" recogida en el art. 2.1.c LOPD respecto a los medios del tratamiento de datos, implicaba ejercer un grado significativo de control y capacidad para dirigir su uso en provecho propio. *Google* entendía que eran los usuarios los que utilizaban sus equipos para acceder al servicio on-line de *Google* Inc, controlaban cada interruptor y botón del equipo, podían conectarlo o desconectarlo de Internet y podían decidir qué servicios usaban y con qué finalidad. Los usuarios tenían control físico sobre el dispositivo y se lo podían llevar a otro país, lo que podría dar lugar, según el criterio de la AEPD, a la aplicación de otra norma de protección de datos. Resolución R/02892/2013 de 18 de diciembre de 2013, PS/00345/2013, Antecedente 7.

[1447] Así, siguiendo con las alegaciones que realizaba *Google* en el procedimiento ante la AEPD esgrimía precisamente como argumento que había que entender que la Directiva 95/46/CE cuando fue aprobada no había podido tener en cuenta ni Internet ni nada parecido a las cookies. El legislador, según *Google*, pretendía aplicar la normativa comunitaria a aquellos responsables no comunitarios que tuviesen centros de proceso de datos en territorio de un Estado miembro de la UE. El considerar los equipos de los usuarios como medios al servicio del responsable conllevaría una aplicación extraterritorial de las normas de los Estados miembros de la UE. *Ibídem*.

doscientos recursos planteados por *Google* contra las resoluciones de la AEPD, que la Audiencia Nacional, órgano remitente de la cuestión prejudicial había suspendido, a la espera de que el TJUE respondiera[1448].

Pues bien, esta aplicación de la sentencia por la Audiencia Nacional es un ejemplo de la fragilidad del concepto de responsable, que si no se interpreta correctamente, al final, consigue el efecto contrario del deseado y la consecuente inseguridad jurídica.

La Audiencia Nacional confunde el criterio comentado del artículo 4.1.a) Directiva 95/46/CE, que sirve para determinar la legislación aplicable, con la aplicación del concepto de responsable del tratamiento.

Al referirse a la aplicación territorial de la normativa de protección de datos, la Audiencia Nacional acoge la interpretación que realiza el TJUE y considera que debe aplicarse el criterio del artículo 4.1.a) Directiva 95/46/CE[1449]. De esta forma, considera a *Google Spain, S.L.* un establecimiento, a los efectos de lo indicado por esta disposición.

Sin embargo, a continuación la Audiencia Nacional responde a la alegación que realiza *Google Spain, S.L.*, referente a su falta de legitimación pasiva, en el procedimiento administrativo seguido ante la AEPD. *Google Spain, S.L.* aduce que la sentencia del TJUE no califica a *Google Spain, S.L.* como responsable del tratamiento y que, aunque su actividad haya sido considerada por el TJUE determinante para aplicar la ley nacional a *Google Inc.*, ésta sociedad es la que gestiona el motor de búsqueda y la que debería eliminar resultados del índice de búsquedas[1450].

La Audiencia Nacional considera que, efectivamente, *Google Inc.* es responsable del tratamiento, pero acude al elemento de corresponsabilidad del concepto para indicar que no es un responsable en solitario, sino que deduce, de lo indicado en la sentencia del

[1448] 226 recursos, según la Memoria de la AEPD de 2013, pág. 31.
[1449] SAN de 29 de diciembre de 2014 (Sala de lo contencioso-administrativo) (ROJ: SAN 4899/2014), FJ 7. Se ha escogido esta sentencia por ser la que resuelve el recurso planteado por *Google* contra la resolución de la AEPD que se refiere a Mario Costeja, asunto que fue el que dio lugar a la cuestión prejudicial resuelta por el TJUE. La fundamentación jurídica referente a la cuestión que se aborda del responsable del tratamiento es la misma en los otros recursos, por lo que se podría transpolar a todos ellos.
[1450] *Ibídem*, FJ 5. De hecho, *Google Spain, S.L.* también se refiere a varias resoluciones de la AEPD en las que ésta consideró responsable a *Google Inc.*, una de ellas es la Resolución R/02892/2013 de 18 de diciembre de 2013, PS/00345/2013, que he mencionado anteriormente, recurrida por *Google*.

TJUE, que *Google Spain, S.L.* también debe ser considerado responsable del tratamiento[1451]. La Audiencia utiliza los argumentos que el TJUE utilizó para considerar aplicable el criterio del artículo 4.1.a) Directiva 95/46/CE para afirmar la responsabilidad de *Google Spain, S.L.*[1452]. La Audiencia deriva esta responsabilidad de la unidad de negocio material y funcional que conforman ambas sociedades (*Google Inc.* y *Google Spain, S.L.*), de forma que la actividad de *Google Spain, S.L.* resulta indispensable para el funcionamiento del motor de búsqueda y, por tanto, ello conlleva que no se pueda excluir su responsabilidad referente al tratamiento de datos[1453].

Además, la Audiencia Nacional acude a otros argumentos para considerar a *Google Spain, S.L.* responsable del tratamiento, como el hecho de que esta empresa haya actuado anteriormente como tal responsable en procedimientos de tutela de derechos seguidos ante al AEPD y en procedimientos ante tribunales españoles[1454]. Si bien, la Audiencia matiza que la postura adoptada por *Google Spain, S.L.*, en esos procedimientos, no debe ser determinante para la cuestión analizada, sí lo considera un indicio importante a los efectos de atribuirle la responsabilidad y aplica la doctrina de los actos propios.

[1451] La Audiencia Nacional acude al concepto de responsable del tratamiento del artículo 2.d) Directiva 95/46/CE, en el que se incluye el elemento de corresponsabilidad, al indicar que la determinación de los fines y los medios del tratamiento de datos se puede hacer "sólo o conjuntamente con otros". Previamente la Audiencia Nacional se refiere también al concepto contenido en el artículo 3.d) LOPD e incluso al que se incluye en el proyecto de Reglamento europeo que sustituirá la Directiva 95/46/CE. También cita el Dictamen 1/2010 del GA29 cuando explica las características del concepto, como su carácter autónomo y funcional y los elementos de los que se compone. SAN de 29 de diciembre de 2014 (Sala de lo contencioso-administrativo) (ROJ: SAN 4899/2014), FJ 5.

[1452] Así se remite la Audiencia Nacional a los apartados 55, 56 y 57 de la sentencia del TJUE relativos a la argumentación sobre el ámbito territorial de la Directiva 95/46/CE. *Ibídem*.

[1453] Según la Audiencia Nacional "carecería de lógica alguna excluir a *Google Spain, S.L.* de cualquier responsabilidad en el tratamiento de los datos personales que lleva a cabo *Google Inc.*, tras afirmar que ese tratamiento se sujeta al Derecho Comunitario precisamente por haberse llevado a cabo en el marco de las actividades de su establecimiento en España, y más aún tras aceptar la relevancia de su participación en la actividad conjuntamente desempeñada por ambas, en relación con el funcionamiento del motor de búsqueda y el servicio que mediante el mismo se presta a los internautas, que conlleva el tratamiento de datos personales que nos ocupa. De no entenderse así se vería menoscabado el efecto útil de la directiva 95/46/CE (...)". *Ibídem*.

[1454] La Audiencia cita, además de algunos procedimientos de tutela seguidos ante la AEPD, en los que podía decirse que había actuado en calidad de responsable, varias sentencias del Tribunal Supremo que no versaban sobre el derecho de protección de datos. Así la STS de 3 de abril de 2012 (Sala 1ª) (ROJ: STS 3942/2012) se refería a cuestiones de propiedad intelectual y la STS de 15 de enero de 2014 (Sala 1ª) (ROJ: STS 69/2014) se refería aL derecho al honor y a la propia imagen. Además la Audiencia Nacional también recurre a la Resolución R/02892/2013 de la AEPD de 18 de diciembre de 2013, PS/00345/2013 que esgrimía *Google Spain, S.L.*, pero para indicar que, en las alegaciones que había hecho *Google Spain, S.L.* en este procedimiento, afirmó que era un activo de *Google Inc.* y cualquier pérdida de *Google Spain, S.L.*, como una multa, se trasladaba de forma automática a *Google Inc.* y que existía un identidad subjetiva entre ambas empresas. *Ibídem.*

Sin perjuicio del mayor o menor acierto de esta argumentación por parte de la Audiencia Nacional relativa a la postura adoptada por *Google Spain, S.L.*, en procedimientos que no son comparables al enjuiciado en la sentencia, lo que merece reproche es que la Audiencia acuda a argumentos de la sentencia del TJUE, utilizados para aplicar el criterio del artículo 4.1.a) Directiva 95/46/CE para calificar a la empresa española como responsable. Estos argumentos no pueden ser los utilizados para calificar a *Google Spain, S.L.* de responsable del tratamiento porque entonces se pierden de vista los elementos que constituyen el concepto y éste pierde su razón de ser.

A mayor abundamiento, se puede hacer mención de la guía publicada por el GA29 sobre los criterios para aplicar la sentencia del TJUE sobre *Google*[1455]. En este documento, el GA29 recuerda que la Directiva 95/46/CE no incluye ninguna referencia sobre la responsabilidad que tiene los establecimientos del responsable, localizados en el territorio de los Estados miembros de la UE[1456]. Sin embargo, para poder aplicar lo establecido en la sentencia, el GA29 estima imprescindible que los titulares de los datos puedan acudir a estos establecimientos, ubicados en los países donde residen, para ejercer sus derechos, al igual que también las autoridades de control pueden contactar con estos establecimientos respecto a denuncias que puedan realizar los titulares de datos.

3. EL RESPONSABLE COMO VÍCTIMA DE LAS DEBILIDADES DE LA REGULACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS

La regulación del derecho a la protección de datos de carácter personal es objeto de reforma, ya que es evidente que nació en un entorno que dista mucho del panorama tecnológico actual. Mientras estas reformas se llevan a cabo, el responsable se configura como una víctima de esta tensión entre realidad y legislación. Además, como se verá el problema irá más allá de lo que el legislador puede afrontar, ya que se mezclan cuestiones políticas y tradiciones jurídicas.

[1455] *Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12, 14/EN WP 225, 26.11.2014, Article 29 Data Protection Working Party.*

[1456] *Ibídem,* págs. 7 a 8.

En este apartado se recorrerán algunas de estas dificultades a las que tiene que enfrentarse el responsable. El primer aspecto al que me aproximaré será el de la rigidez de la regulación de las transferencias internacionales en la Directiva 95/46/CE y la normativa que la transpone, si bien también resaltaré los esfuerzos que las autoridades realizan para intentar flexibilizar de algún modo esta regulación. Posteriormente señalaré las diferencias entre los sistemas jurídicos continentales y anglosajones, que se reflejan en el sistema de *pre-trial discovery* estadounidense o la vigilancia masiva. La regulación del derecho a la protección de datos se ve incapaz de cumplir con su cometido de proteger los datos de los ciudadanos europeos y esta incapacidad se suple con la asignación de obligaciones, que dificultan el uso de las tecnologías, por parte de los responsables europeos y que los sitúan, por tanto, en desventaja frente a operadores de otros países.

3.1. El responsable ante la rigidez de la regulación de las transferencias internacionales en el contexto digital

3.1.1. La rigidez de la regulación de las transferencias internacionales y el esfuerzo de las autoridades por introducir mecanismos más flexibles

Cuando se abordó el régimen de las transferencias internacionales, se pudo ver que es especialmente estricto, ya que establece, en principio, una regla general de prohibición, cuando estas transmisiones se quieren realizar a países terceros, que se considera que no cumplen con el nivel adecuado de protección de los datos. Este nivel lo determina la Comisión o las autoridades de control. Y si bien se ha establecido un listado de excepciones a esta prohibición, las autoridades desincentivan su utilización, excepto en casos puntuales. Por tanto, la principal vía que queda para poder llevar a cabo las transferencias es a través de la tramitación de autorizaciones que otorgan las autoridades de control.

La Directiva 95/46/CE pretendía conseguir la armonización de las legislaciones en materia de protección de datos, con el fin de facilitar la libre circulación en el mercado interior europeo. Sin embargo, el margen de maniobra que la Directiva 95/46/CE otorgaba a los Estados miembros, junto con la aplicación incorrecta de la misma, han ocasionado divergencias entre las legislaciones nacionales, que transponen la Directiva

95/46/CE[1457]. Esto ha ocasionado que se contradiga el objetivo de libre circulación y que los responsables que están establecidos en varios Estados miembros tengan que hacer un esfuerzo por adaptarse a estas normativas diferentes[1458].

El modelo regulatorio de las transferencias en la Directiva 95/46/CE se creó en un contexto tecnológico que nada tiene que ver con el actual, como ya hemos visto. La globalización y la tecnología permiten que se puedan contratar servicios a empresas, que pueden estar ubicadas en cualquier punto del planeta, que implican servicios en capas que pueden prestar una multitud de participantes de forma automática. Por tanto, la limitación geográfica ha desaparecido pero los operadores europeos se ven constreñidos por una limitación legal.

Para cumplir con los requisitos que les imponen las veintiocho legislaciones nacionales de protección de datos, las empresas europeas requieren de la necesaria colaboración de los prestadores ubicados en países fuera del EEE. Esta colaboración dependerá de la voluntad de estos prestadores, ya que la normativa de protección de datos no les hace claramente responsables del incumplimiento a ellos, sino a las empresas europeas.

Las empresas europeas quieren utilizar estos servicios que disminuyen sus costes y las compañías tecnológicas, que surgen en Europa y que quieren prestar también este tipo de servicios, precisan realizar estas transferencias internacionales para llevar a cabo estos negocios que podrían contribuir al desarrollo económico de la UE ¿Cómo asegurar la protección de datos sin mermar la capacidad competitiva de las empresas europeas?

Las autoridades de protección de datos europeas, como se ha indicado anteriormente, han insistido en que el cliente de este tipo de servicios, en calidad de responsable es quien debe asegurarse que se cumpla con la normativa de protección de datos. Por tanto, si las condiciones contractuales del servicio no incluyen todos los aspectos necesarios que permitan que el cliente pueda solicitar la autorización para

[1457] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, un enfoque global de la protección de los datos personales en la Unión Europea, COM(2010) 609 final, Bruselas, 4.11.2010, pág. 11.
[1458] *Ibídem.*

realizar las transferencias internacionales o ni siquiera conoce estas transferencias, no deberá contratar el servicio.

Pese a esta postura, las autoridades trabajan en posibles mecanismos que faciliten de alguna manera que los proveedores de estos servicios -principalmente pensando en los proveedores europeos- puedan tener un papel más proactivo en el cumplimiento de la legislación[1459]. Ejemplo de ello es la creación, por el GA29, de las *Binding Processor Rules* o reglas corporativas vinculantes (BPR) para encargados del tratamiento, que son una respuesta al aumento del volumen y de la complejidad de las transferencias internacionales de datos derivado, precisamente, de la globalización, la ubicación de los centros de datos y el *cloud computing*[1460]. Al igual que sus predecesoras, las *Binding Corporate Rules* o reglas corporativas vinculantes (BCR) destinadas para organizaciones multinacionales, las BPR tienen como objetivo facilitar las transferencias de datos en el marco de la organización del encargado del tratamiento que actúa para un determinado responsable del tratamiento europeo.

Hay que poner de relieve el papel de la AEPD en este ámbito que, como ya se comentó, ha impulsado la elaboración de cláusulas contractuales que permiten a encargados del tratamiento presentar una solicitud de autorización que le permita subcontratar a otras empresas que estén en países que no cuenten con nivel adecuado de protección. De esta forma este encargado proveedor de servicios puede facilitar a sus clientes, los responsables, el trámite de solicitud de autorización, de forma que bastará una notificación a la AEPD y la remisión al trámite previo realizado por el encargado. Estas cláusulas han derivado en una propuesta del GA29 a la Comisión para que esta institución las adopte y así puedan utilizarlas todas las autoridades[1461]. Asimismo, la AEPD adaptó este sistema contractual al entorno del *cloud computing*, en virtud de las garantías que había especificado el GA29[1462].

[1459] Ver Capítulos V y VI.

[1460] Documento explicativo sobre las normas corporativas vinculantes para los encargados del tratamiento, *op. cit.*, pág. 5.

[1461] *Working document 1/2014 on draft ad hoc contractual clauses "EU data processor to non-EU sub-processor", op.cit*..

[1462] Según lo indicado en su Dictamen 5/2012 sobre la computación en nube, *op.cit.*. De esta forma, se acepta que se modulen algunas de las obligaciones establecidas en la Decisión 2010/87/UE, como la obligación de auditoría. En la Decisión de la Comisión el importador de datos debe permitir que el exportador realice una auditoría en sus instalaciones (cláusulas 5.f y 12.2 Decisión 2010/87/UE). El GA29 y la AEPD indican que será posible que se realicen auditorías por terceros independientes seleccionados por

3.1.2. El responsable y las dudas sobre la validez de la Decisión Safe Harbour

Hasta ahora se ha hecho referencia a los supuestos de transferencias internacionales a países que no cuenten con el nivel adecuado de protección. Sin embargo, cuando la transferencia sea a EEUU, un país de nivel adecuado si la empresa importadora de los datos se ha acogido a los principios de la Decisión *Safe Harbour*, no por ello, la empresa exportadora europea tendrá la seguridad jurídica que cabría esperar.

La Decisión *Safe Harbour* ya había recibido críticas que ponían en duda su adecuada aplicación por el gobierno y las empresas estadounidenses que se acogían a la misma[1463]. El GA29 había indicado las limitaciones de la Decisión, en el marco de los nuevos entornos tecnológicos, como el de *cloud computing*, en el que podían ser necesarias medidas adicionales de protección[1464]. En este ámbito, el GA29 indicó que "la autocertificación con puerto seguro por sí sola no puede considerarse suficiente". Por tanto, el GA29 estimaba que era necesario que el responsable del tratamiento europeo, que quisiera transferir datos a una empresa acogida a la Decisión *Safe Harbour*, solicitara pruebas de que ésta tenía una certificación acorde con la Decisión y de que cumplía sus

---

el proveedor de servicios y que se proporcione acceso al informe de auditoría al cliente. Otra modulación que sugiere el GA29 y que la AEPD incorpora es sobre la subcontratación (cláusula 11.1 Decisión 2010/87/UE). De esta forma, la rigidez de la Decisión se suaviza para permitir que en caso de subcontratación se pueda suscribir un único contrato con cada subcontratista y no tener que suscribir un contrato con cada cliente para cumplir con la obligación de solicitar el consentimiento previo de éste a cada uno de los subcontratistas. Además se establece la necesidad de identificar a los subcontratistas y su ubicación mediante su publicación en un sitio web y la previsión de que se pueda finalizar el contrato en caso de que el cliente no estuviera de acuerdo con esta subcontratación.

[1463] Ya en un estudio realizado en el año 2004 por el CRID se alertaba de algunas deficiencias en la aplicación de esta decisión. Especialmente se indicaba en el estudio que las entidades estadounidenses analizadas tenían dificultades para trasladar los principios de la Decisión S*afe Harbour* a sus políticas internas de tratamiento de datos, como resultado de la falta de conocimiento acerca de de las obligaciones que estos principios comportan y de una percepción diferente de lo que implica la protección de datos. Además, entre los aspectos destacados respecto a los principios que se establecen en la decisión, se indica que son las compañías las que, al solicitar la certificación de *Safe Harbour*, deben seleccionar si actúan en calidad de responsables del tratamiento o de encargados del tratamiento. De acuerdo con las conclusiones del estudio se recomendaba que se proporcionara más información a estas entidades sobre la diferenciación entre ambos roles. J. DHONT, M.V. PÉREZ ASINARI, Y. POULLET (*Centre de Recherche Informatique et Droit, University of Namur, Belgium*), J.R. REIDENBERG (*Fordham University School of Law, New York, USA*), L.A. BYGRAVE (*Norwegian Researc Centre for Computers and Law, University of Oslo, Norway*), *Safe harbour decision implementation study, at the request of the European Commission, Internal Market DG, Contract PRS/2003/A0-7002/E/27*, 2004, págs. 105 y 108, http://ec.europa.eu/justice/policies/privacy/docs/studies/safe-harbour-2004_en.pdf (fecha consulta: 23.7.2013).

[1464] Dictamen 5/2012 sobre la computación en nube, WP 196, 01037/12/ES, 1.7.2012, Grupo de trabajo Artículo 29 sobre la protección de datos, pág. 26.

principios[1465]. Estas inquietudes por parte de las autoridades de control respecto a la efectividad de la decisión se elevaron como consecuencia de las filtraciones sobre espionaje en EEUU[1466].

Hay que tener en cuenta que las empresas involucradas en el programa PRISM de espionaje, eran empresas que contaban con la certificación de la Decisión *Safe Harbour*[1467]. En consecuencia, el Parlamento Europeo pidió a la Comisión la suspensión de la Decisión *Safe Harbour* y solicitó a las autoridades de control que utilizaran sus potestades para evitar que las transferencias se realizaran, en virtud de este instrumento[1468].

Ante estas filtraciones, el GA29 también alertó a la Comisión Europea sobre la vulneración del derecho de protección de datos e indicó las dudas sobre el cumplimiento de la Decisión *Safe Harbour*[1469]. El GA29 recordaba que la Decisión *Safe Harbour* establece una serie de excepciones a la aplicación de los principios: si lo justifican las

[1465] Dictamen 5/2012 sobre la computación en nube, *op. cit*, pág. 20.

[1466] Se ilustran estas inquietudes con la decisión publicada por las autoridades de control alemanas en la que pedían a los responsables europeos que transfiriesen datos a EEUU que comprobaran si las entidades estadounidenses cumplían realmente con los principios de puerto seguro y establecían que como mínimo se verificara si la certificación seguía siendo válida. El 24 de julio de 2013, a raíz de las revelaciones sobre el espionaje llevado a cabo por EEUU, las autoridades alemanas fueron más lejos y afirmaron que existía gran probabilidad de que se estuvieran infringiendo los principios de la decisión. Algunas de estas autoridades (como la de Bremen) solicitaron a los exportadores de datos alemanes que les notificaran si los proveedores estadounidenses a quienes proporcionaban datos impedían a la NSA (la Agencia Nacional de Seguridad de EEUU) el acceso a los mismos. Además la autoridad de control irlandesa había descartado investigar varias denuncias contra la validez de los principios de *safe harbour* a raíz de las revelaciones de espionaje y el Tribunal Supremo de Irlanda había admitido a trámite la solicitud de control jurisdiccional para examinar esta inacción de la autoridad de protección de datos. Ver Decisión *Düsseldorfer Kreis* de 28/29 de abril de 2010. *Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich* de 28/29 de abril 2010, Hannover: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__bl. y resolución de la Conferencia alemana de comisarios encargados de la protección de datos, http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870, ambos citados en la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, COM(2013) 847 final, Bruselas, 27.11.2013, págs. 5 a 6.

[1467] Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, *op.cit*., pág. 17.

[1468] Resolución del Parlamento Europeo, de 12 de marzo de 2014, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EEUU, los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de justicia y asuntos de interior, P7_TA-PROV(2014)0239.

[1469] Carta del GA29, de 13 de agosto de 2013, a la Vicepresidenta de la Comisión Europea, Viviane Reding. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130813_letter_to_vp_reding_final_en.pdf (fecha consulta: 23.7.2013).

exigencias de seguridad nacional, interés público y el cumplimiento de una ley, o por disposición legal o reglamentaria o jurisprudencia[1470]. Sin embargo, el Grupo ponía en duda que la vigilancia masiva que había salido a la luz se pudiera considerar incluida en estas excepciones que debían interpretarse de forma estricta y sujetarse a criterios de proporcionalidad[1471].

A finales de 2013, la Comisión Europea publicaba un memorándum sobre los pasos que se iban a llevar a cabo para restaurar la confianza en las transferencias de datos entre EEUU y la UE[1472]. En el mismo, la Comisión realizaba unas recomendaciones para mejorar el funcionamiento de la Decisión *Safe Harbour* y que debían cumplir las autoridades y las empresas estadounidenses adheridas a los principios[1473].

Entre estas recomendaciones, la Comisión indicó que era necesario que las empresas adheridas a la Decisión incluyeran en sus políticas de privacidad información sobre los supuestos en los que harían uso de las excepciones para cumplir con las limitaciones indicadas y la importancia de que la excepción relativa a la seguridad nacional se usara sólo si era estrictamente necesario o proporcionado[1474].

Como recalcó la Comisión, las excepciones mencionadas de la Decisión *Safe Harbour* debían interpretarse restrictivamente, además de cumplir con lo preceptuado por el CEDH y la jurisprudencia del TEDH[1475]. No se podía prever en el año 2000, cuando se aprobó esta decisión, el acceso a gran escala de las agencias de inteligencia a los datos transferidos, en virtud de la misma.

[1470] Decisión *Safe Harbour,* Anexo I.

[1471] Carta del GA29, de 13 de agosto de 2013, a la Vicepresidenta de la Comisión Europea, Viviane Reding. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130813_letter_to_vp_reding_final_en.pdf (fecha consulta: 23.7.2013).

[1472] *Restoring trust in EU-US data flows-Frequently Asked Questions, European Commission MEMO/13/1059, 27.11.2013, Brussels*. http://europa.eu/rapid/press-release_MEMO-13-1059_es.htm, (fecha consulta: 2.11.2014).

[1473] *Ibídem.*

[1474] Incluía como ejemplo de esta información que podían incluir estas empresas la que publicaba Nokia: "Relatively transparent information in this respect is provided by some European companies in Safe Harbour. For example Nokia, which has operations in the U.S. and is a Safe Harbour member provides a following notice in its privacy policy: "We may be obligated by mandatory law to disclose your personal data to certain authorities or other third parties, for example, to law enforcement agencies in the countries where we or third parties acting on our behalf operate."" *Ibídem*.

[1475] Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, *op.cit*., pág. 18.

Pero ¿cómo afecta esta falta de confianza en la Decisión *Safe Harbour* a los responsables europeos? ¿Pueden seguir realizando transferencias a empresas adheridas a la misma? Ya se ha comentado las dudas del GA29 que exige un plus a estos responsables en su diligencia cuando quieran llevar a cabo estas transmisiones en el ámbito del *cloud computing*.

El 25 de julio de 2014 la *High Court of Ireland* interpuso una cuestión prejudicial, en el marco de un litigio que enfrentaba a un ciudadano austríaco contra la autoridad de control de Irlanda[1476]. Lo que se cuestionaba era si la autoridad de control, al conocer que se realizaba una transmisión de datos a EEUU, cuya legislación y práctica no prevén supuestamente una protección adecuada de la persona sobre la que versan los datos, ¿debía aceptar que se aplica la Decisión *Safe Harbour* sin ahondar más o debía realizar su propia investigación del asunto a la luz de los hechos acaecidos desde que en el año 2000 se adoptó esta Decisión?

A la espera de resolver estas dudas sobre la efectiva protección de los ciudadanos europeos, no parece lo más acertado que se requiera a los responsables europeos para que suplan la falta de protección con una mayor diligencia. Es cierto que se trata de una

[1476] Petición de decisión prejudicial planteada por la *High Court of Ireland* (Irlanda) el 25 de julio de 2014, *Maximillian Schrems/Data Protection Commissioner*, C-362/14, DO C 351 de 6.10.2014. Las conclusiones del Abogado General se conocerán el 23 de septiembre de 2015. Parece ser que, inicialmente las conclusiones debían emitirse el 24 de junio. En este caso, el sr. Schrems pretendía que la autoridad de control irlandesa suspendiera las transferencias de datos que realizaba *Facebook* a EEUU. *Facebook* estaba acogida a la Decisión *Safe Harbour*. *Europe's Highest Court delays decisión in safe harbor case Schrems vs. Facebook*, 10.6.2015, Hunton&Williams LLP, 2015, https://www.huntonprivacyblog.com/2015/06/10/europes-highest-court-delays-decision-safe-harbor-case-schrems-vs-facebook/ (fecha consulta: 9.9.2015). El sr. Schrems ya había protagonizado una acción contra *Facebook*, ante la autoridad de control irlandesa que finalmente dio la razón a Schrems y que hizo que *Facebook* hiciera algunos cambios en sus prácticas. La red social, ante la petición de este ciudadano austríaco, le proporcionó los datos que sobre él tenía de su actividad de tres años en la red social y que llenaron 1.222 páginas que incluían información detallada sobre todas las acciones realizadas por el usuario e incluso mensajes que este había borrado. "Un estudiante fuerza a Facebook a mejorar la privacidad", El País Tecnología, 25.12.2011, http://tecnologia.elpais.com/tecnologia/2011/12/25/actualidad/1324807261_850215.html (fecha consulta: 9.9.2015). Asimismo, el sr. Schrems inició una acción colectiva contra *Facebook* por daños y perjuicios ocasionados al considerar que la red social había vulnerado su derecho a la privacidad, al ayudar a la Agencia de Seguridad Nacional de EEUU, mediante la información a la que accedió esta Agencia, en virtud de los programas de espionaje. "Un estudiante lidera una demanda colectiva global contra Facebook" ABC Tecnología, Reuters, 3.8.2014, http://www.abc.es/tecnologia/redes/20140801/abci-estudiante-austriaco-demanda-global-201408011256.html, (fecha consulta: 9.9.2015). En julio de 2015 se conocía que los tribunales de Viena no habían admitido la demanda por motivos formales, pero que se iba a recurrir. http://europe-v-facebook.org/EN/en.html (fecha consulta: 9.9.2015).

cuestión compleja de resolver, en la que intervienen cuestiones políticas pero la solución, no puede consistir en hacer recaer el peso del problema en las espaldas del responsable.

La AEPD, en su 4ª jornada abierta de 27 de abril de 2012, dedicada al *cloud computing*, ante las dudas suscitadas sobre la Decisión, en respuesta a una pregunta que se realizó sobre la contratación de un proveedor de *cloud computing*, con domicilio en EEUU, adherido a la Decisión *Safe Harbour*, recordó que estas entidades tienen reconocido el nivel adecuado de protección[1477]. Asimismo, la ACPD, en algunos dictámenes relativos a servicios de *cloud computing* también confirma la validez de las transferencias a entidades adheridas a la Decisión[1478].

3.2. Las diferencias entre sistemas jurídicos y la vigilancia masiva

3.2.1. El responsable ante las diferencias de los sistemas jurídicos y su difícil encaje con el respeto a la protección de datos: el pre-trial discovery

En el contexto global tecnológico que se ha descrito, el responsable debe lidiar con las diferencias de sistemas jurídicos, como son, el del *Common Law* y el continental europeo. Una de estas diferencias es la relativa a la fase de *pre-trial discovery*. En esta etapa del procedimiento judicial, en el sistema anglosajón, se persigue el descubrimiento de pruebas. Es una fase preparatoria que se fundamenta en asegurar la obtención del máximo de información, que puede estar en poder de la parte contraria o de terceros. En los EEUU el ámbito de esta etapa es muy amplio, de forma que la legislación federal y estatal incentiva este intercambio de información que incluye, no sólo información directamente relacionada con el asunto, sino información que podría llevar al descubrimiento de otros datos que sí fueran relevantes (lo que se conoce como *fishing expeditions*)[1479].

[1477] También lo indica sin más en su Guía para clientes que contraten servicios de *Cloud Computing*, *op. cit.*, pág. 15.
[1478] La ACPD indica en sus informes que la adhesión a la Decisión *Safe Harbour* supone "a fecha de hoy" que los datos transmitidos serán tratados con determinadas garantías y condiciones de seguridad. Sin embargo, explica toda la problemática suscitada a raíz del espionaje. Ver Dictamen CNS-27/2014 de la ACPD, apdo. IV.
[1479] *Working Document 1/2009 on pre-trial discovery for cross border civil litigation, 00339/09/EN WP 158, adopted on 11.2.2009, Article 29 Data Protection Working Party*, págs. 3 y 4.

Las empresas con sede o con algún establecimiento en EEUU se verán sujetas a esta obligación. Pero no sólo estas empresas se ven afectadas. En modelos de negocio como los de *cloud computing*, los prestadores de servicios que son estadounidenses podrán verse compelidos a entregar información almacenada en sus servidores de sus clientes.

El GA29 advertía de esta tensión existente entre la obligación de comunicar datos establecida en las normas procesales estadounidenses, durante el *pre-trial discovery* y la aplicación de la normativa de protección de datos. El Grupo indicaba que únicamente podía proporcionar unas pautas acerca de estas cuestiones, ya que la solución quedaba fuera de su ámbito porque sólo podría resolverse a nivel nacional[1480].

El GA29 señalaba el contraste de este sistema con los de tradición continental, de forma que citaba específicamente los modelos francés y español en los que se restringe la comunicación de los documentos admitidos en un juicio, de forma que esto lo supervisa el juez, que decide si estos documentos son admisibles o no. Asimismo, algunos de estos países disponen de leyes que pretenden el bloqueo de la entrega de información a otros países, como Francia[1481].

Si bien existe el Convenio de La Haya sobre la obtención de pruebas en el extranjero en materia civil o comercial de 18 de marzo de 1970, algunos países como España, efectuaron reservas mediante las que se negaban a aceptar su utilización respecto

[1480] El GA29 sugiere que podría suscribirse acuerdos del estilo del Convenio de La Haya sobre la obtención de pruebas en el extranjero en materia civil o comercial de 18 de marzo de 1970. *Working Document 1/2009 on pre-trial discovery for cross border civil litigation, op.cit.*, pág. 2. Hay que indicar que existen entidades que realizan esfuerzos por superar estas dificultades, como *The Sedona Conference*, que se define como un instituto de investigación y educación, dedicado al estudio de los avances legales y de políticas, en materias como la litigación compleja. Pretende crear un diálogo entre jueces, abogados, expertos, académicos y otros sujetos para conseguir avances en la ley, de una forma razonada. www.thesedonaconference.org (fecha consulta: 29.11.2014). Así por ejemplo, publicó un documento con unos principios internacionales que parten de la idea de que la protección de los datos personales y el proceso de *discovery* deben coexistir, de forma que prenteden hallar un equilibrio entre ambos aspectos. *The Sedona Conference International Principles on Discovery, Disclosure&Data Protection: Best practices, recommendations&principles for addressing the preservation discovery of protected data in U.S. litigation, A project of the Sedona Conference Working Group 6 on International Electronic Information Management, Discovery&Disclosure (WG6), European Union Edition, public comment version, December 2011,* pág. 3.

[1481] En 2008 este país consideró culpable a un abogado al que se sancionó con 10.000 € por haber proporcionado información a los tribunales estadounidenses en el asunto *In re Advocat "Christopher X", Cour de Cassation, December 12, 2007, Appeal No 07-83228*. *Working Document 1/2009 on pre-trial discovery for cross border civil litigation, op. cit.*, pág. 5 y *Comment of The Sedona Conference Working Group 6 to Article 29 Data Protection Working Party Working Document 1/2009 (WP 158),op. cit.* pág. 8.

a este proceso[1482]. La tensión va más allá del derecho a la protección de datos y los tribunales estadounidenses entienden que el Convenio de La Haya es una vía opcional a la que pueden recurrir pero no tienen porque seguirla[1483].

Para mostrar la complejidad a la que se enfrenta el responsable, baste citar algunos aspectos que el responsable debería tener en cuenta a la hora de proporcionar los datos que se le soliciten en virtud de una petición de *discovery*. Respecto a la legitimación del tratamiento de datos, el GA29 considera tres posibles bases jurídicas: el consentimiento, el cumplimiento con una obligación legal (art. 7.c Directiva 95/46/CE) o el interés legítimo (art. 7.f Directiva 95/46/CE).

El consentimiento será difícilmente la base ideal y el cumplimiento de una obligación legal tampoco, ya que, en este caso, la obligación viene de una normativa extranjera[1484], por lo que deberá acudirse a la base relativa al interés legítimo. En este caso, el responsable, como ya se ha analizado, debe ponderar su interés por cumplir con la normativa estadounidense y los intereses, derechos y libertades de los afectados, que no tendrán seguramente ninguna relación con el proceso judicial. En esta ponderación, el responsable también debe valorar la adopción de medidas adicionales de protección y el reconocimiento del derecho de oposición, que establece el artículo 14 Directiva 95/46/CE. El GA29 recomienda, en este sentido, la restricción de la comunicación de datos a lo mínimo imprescindible y si fuera posible, anonimizar estos datos, lo que puede llevarse a cabo por un tercero de confianza, que se ubique en la UE.

Se enlaza además esta recomendación con el cumplimiento de los principios de calidad (art. 6 Directiva 95/46/CE). El GA29 recuerda la obligación del responsable de valorar y limitar los datos que debe proporcionar[1485]. De esta manera, estima que el

[1482] Se cita esta reserva a modo de ejemplo: "Reserva D. A tenor del artículo 23, España no acepta las comisiones rogatorias derivadas del procedimiento "*pre-trial discovery of documents*" conocido en los países del *common law*". Instrumento de ratificación del Convenio relativo a la obtención de pruebas en el extranjero en materia civil o mercantil, hecho en La Haya el 18 de marzo de 1970 (BOE núm. 203 de 25.8.1987).

[1483] *Société Nationale Industrielle Aérospatiale v United States District Court, 482 U.S. 522, 544 n.28 (1987)*, citado en *Working Document 1/2009 on pre-trial discovery for cross border civil litigation, op. cit.*, pág. 7.

[1484] Si bien matiza el GA29 que podría ser que algún Estado miembro contemplara la obligatoriedad de cumplir con este proceso, por lo que entonces sí sería válida. *Working Document 1/2009 on pre-trial discovery for cross border civil litigation, op. cit., págs.* 8 a 10.

[1485] *Working Document 1/2009 on pre-trial discovery for cross border civil litigation, op. cit.*, pág. 11.

responsable debe considerar si es necesario proporcionar los datos personales o se pueden eliminar. Esta valoración puede ser difícil y debe realizarse en un corto intervalo de tiempo, por lo que el GA29 sugiere acudir a expertos en el proceso de *discovery*, terceros de confianza que sean independientes para poder adoptar esta decisión sobre la pertinencia de la información a comunicar. También anima a los responsables a implicar a los "Encargados de protección de datos" en el proceso y a aproximarse a los tribunales estadounidenses para explicar sus obligaciones legales, en materia de protección de datos.

La AEPD publicó un informe mediante el que respondía a una empresa a la que se había solicitado información, en virtud de este proceso de *discovery*[1486]. En el mismo, la AEPD aplicaba los criterios establecidos por el GA29. La empresa consultante debía entregar información que incluía datos personales de sus empleados. La AEPD consideró que esta compañía ostentaba un interés legítimo en realizar este tratamiento de datos, que tenía su fundamento en el derecho a la tutela efectiva (art. 24 CE) y en su derecho a la defensa. En la ponderación que había que realizar para ver si este interés legítimo debía prevalecer sobre el derecho de los empleados de protección de datos, la AEPD consideró que se cumplía con los principios de proporcionalidad y transparencia[1487]. Asimismo, la AEPD también tenía en cuenta que la solicitud la respondía directamente el requerido. La transferencia internacional de datos que se originaba se consideró que tenía su fundamento en una de las excepciones previstas en la LOPD, que permitía que se realizara cuando sea precisara para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial (art. 34.i LOPD).

3.2.2. El responsable víctima de la imposibilidad de proteger los derechos ante la vigilancia masiva de los gobiernos

El responsable, además de tener que hacer frente, como se ha visto, a las diversidades de los sistemas judiciales de los diferentes países, también es víctima del abuso por ciertos países de las capacidades de vigilancia de las nuevas tecnologías. Hay

[1486] Informe 0469/2011 de la AEPD.

[1487] La proporcionalidad que correponde con el cumplimiento del principio de calidad (art. 4.1 LOPD) se cumpliría, ya que la empresa realiza un proceso de filtrado de los datos y contrata a un tercero, para que realice un proceso para extraer aquellos datos personales que no sean relevantes para la petición. La transparencia se cumple, al informar a los empleados del proceso. *Ibídem*.

que diferenciar si el sistema de vigilancia es el de un Estado miembro o el de un país tercero.

Los programas de vigilancia de los Estados miembros no estarían sometidos a la Directiva 95/46/CE, en virtud de la exclusión referida a aquellos tratamientos de datos que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal (art. 3.2 Directiva 95/46/CE). No obstante, pese a que no se pueda aplicar la normativa europea a esta materia, el GA29 recuerda que los Estados miembros deben tener en cuenta el CEDH y el Convenio 108[1488].

La sentencia del TJUE que invalidó la directiva de conservación de datos señaló que la captación masiva de información, sin discriminar, sería, en principio, contraria al principio de proporcionalidad, necesario en el establecimiento de límites a los derechos de vida privada y de protección de datos (arts. 7, 8 y 52.1 Carta UE)[1489]. El TJUE estimó que era especialmente grave que la conservación y utilización de los datos se efectuasen sin que el usuario hubiera sido informado, de forma que podía generar el sentimiento de que su vida privada era objeto de vigilancia constante[1490].

En este sentido, cabe recordar el asunto *SWIFT*, en el que la autoridad de protección de datos belga consideró, que esta empresa de mensajería financiera llevó a cabo "una violación oculta, sistemática, masiva y de larga duración de los principios europeos fundamentales en lo relativo a la protección de datos", al decidir proporcionar información de ciudadanos europeos a las autoridades estadounidenses, en virtud de citaciones administrativas[1491].

[1488] *Opinion 4/2014 on surveillance of electronic communications for intelligence and national security purposes, 819/14/EN WP 215, 10.4.2014, Article 29 Working Party*, págs. 6, 13 a 14.

[1489] Sentencia del TJUE de 8 de abril de 2014, *Digital Rights Ireland* y *Seitlinger* y otros, C-293/12 y C-594/12, EU:C:2014:238, apdo. 60.

[1490] *Ibídem*, apdo. 37.

[1491] Así, el GA29, al examinar la legitimación del tratamiento de datos realizado por SWIFT consideró inicialmente que tendría un interés legítimo en cumplir con las citaciones (*subpoenas*) conforme a la legislación estadounidense porque, en caso contrario, enfrentaría una posible sanción. Sin embargo, el GA29 estimó finalmente que ello no podía prevalecer sobre el interés o los derechos y libertades fundamentales de los numerosos interesados afectados (SWIFT según su informe anual de 2005 procesaba una media de 12 millones de mensajes a diario). Dictamen 10/2006 sobre el tratamiento de datos personales por parte de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (*Worldwide Interbank Financial Telecommunication*-SWIFT), *op. cit.*, págs. 8, 21 a 22.

En ambas situaciones, se recalcó la gravedad de la vulneración de los derechos por el carácter indiscriminado, el gran volumen de información y la ocultación de su uso.

Como indica el GA29, ni siquiera aquellos ciudadanos más cuidadosos en su devenir *online,* pueden protegerse de los programas de vigilancia masiva[1492]. Esta impotencia de los ciudadanos ante esta invasión es contra la que se debe luchar. Evidentemente, la seguridad de estos mismos ciudadanos también es un valor a proteger, pero no a cualquier precio.

Y es que un estudio sobre los sistemas de vigilancia en cinco Estados miembros (Reino Unido, Suecia, Francia, Alemania y Holanda) mostró que, aunque los recursos empleados no se podían comparar con los de EEUU (excepto los de Reino Unido), en todos ellos, excepto en uno (Países Bajos), se realizaban prácticas de "*upstreaming*", es decir, de interceptación directa de datos a través de la infraestructura de telecomunicaciones[1493]. En este estudio se resaltó que los servicios de inteligencia no habían respondido a las acusaciones que se les habían realizado y que durante la elaboración del mismo, sus autores se encontraron con la actitud de secretismo entorno a los objetivos de la vigilancia y la forma en la que se trataban los datos. El estudio, por tanto, planteaba la necesidad de revisar la responsabilidad de estos servicios de espionaje y la participación de los colaboradores del sector privado[1494].

Respecto a los programas de vigilancia de países terceros no sería aplicable esta exclusión relativa a la seguridad nacional, ya que ésta sólo puede ser utilizada por los Estados miembros. Por tanto, se aplicaría en principio la regulación de la Directiva 95/46/CE a las transmisiones de datos realizados desde Europa y utilizadas para el fin de espionaje de países terceros[1495]. Asimismo, el GA29 ya ha avisado que ninguno de los instrumentos disponibles que permiten realizar una transferencia internacional de datos (la Decisión *Safe Harbour*, los modelos de cláusulas contractuales y las BCR) permiten

[1492] *Opinion 4/2014 on surveillance of electronic communications for intelligence and national security purposes, op. cit.*, pág. 6.
[1493] *National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law, Study. Directorate-General for Internal Policies, Policy Department C, Citizen's rights and Constitutional Affairs, European Parliament, PE 493.032, October 2013,* pág. 5.
[1494] *Ibídem.*
[1495] *Opinion 4/2014 on surveillance of electronic communications for intelligence and national security purposes*, pág. 7.

que autoridades públicas de países terceros accedan a datos personales con fines de vigilancia indiscriminada y masiva. La utilización de estos instrumentos no puede significar una menor protección que si los datos no salieran de la UE[1496]. Ya se ha mencionado, en este sentido, las excepciones que contempla, por ejemplo, la Decisión *Safe Harbour*, pero insistió el GA29 en que estas excepciones deben ser interpretadas de forma restrictiva, es decir, sólo se podrían utilizar para supuestos concretos y puntuales[1497]. También hay que recordar la cuestión prejudicial planteada ante el TJUE relativa a la validez de la Decisión *Safe Harbour*[1498].

Desde el 29 de marzo de 2011, la UE y los EEUU negociaban un acuerdo marco, conocido como el *Data Protection Umbrella Agreement,* que tenía como objetivo asegurar la protección de los datos de los ciudadanos europeos que debían transmitirse a EEUU, con fines de prevención, detección, investigación y persecución de delitos. Las negociaciones se dieron por finalizadas en septiembre de 2015 aunque la aprobación del mismo queda pendiente de la adopción de una ley que está en tramitación en el Congreso de EEUU y que permitirá que los ciudadanos europeos puedan acudir a los tribunales estadounidenses[1499].

Si bien, el GA29 veía este acuerdo como algo positivo también señalaba sus limitaciones. Como este acuerdo se adopta en virtud del derecho de la UE, de nuevo no tendrá en cuenta el tema de la seguridad nacional y el GA29 deduce que no se referirá a entidades privadas, sino que sólo afectará a transmisiones de datos entre entidades públicas. Por tanto, el GA29 estima que no será suficiente para proteger a los ciudadanos y haría falta un acuerdo internacional específico para esta protección frente a la vigilancia masiva que deberían negociar los Estados miembros.

[1496] *Ibídem.*
[1497] *Ibídem.*
[1498] Petición de decisión prejudicial planteada por la *High Court of Ireland* (Irlanda) el 25 de julio de 2014, *Maximillian Schrems/Data Protection Commissioner*, C-362/14, DO C 351 de 6.10.2014.
[1499] Este era el principal obstáculo que impedía que las partes llegaran a un acuerdo: garantizar a los ciudadanos europeos que no residan en EEUU puedan acudir a los tribunales de este país en las mismas condiciones que lo hacen los ciudadanos estadounidenses. *Factsheet EU-US negotiations on data protection, European Commission, June 2014,* http://ec.europa.eu/justice/data-protection/files/factsheets/umbrella_factsheet_en.pdf, (fecha consulta: 2.11.2014). El 8 de septiembre de 2015 la Comisaria europea Vera Jourová informaba de la finalización de las negociaciones. La firma del acuerdo quedaba pendiente de que se aprobara la ley en el Congreso estadounidense (la *Judicial Redress Bill*), http://europa.eu/rapid/press-release_STATEMENT-15-5610_en.htm (fecha consulta: 9.9.2015).

Hay que decir que en EEUU se insiste en aprovechar la información para luchar contra la ciberdelincuencia. Para ello, se quieren aprovechar todos los datos que puedan extraer, no sólo las entidades gubernamentales, sino también los operadores privados. La mezcla de lo público y lo privado se ejemplifica con el proyecto de ley estadounidense denominado *Cybersecurity Information Sharing Act* o CISA, que puede traducirse como ley de intercambio de información sobre ciberseguridad.

Este proyecto de ley se presentó al Senado estadounidense el 7 de octubre de 2014, más de un año después de que se bloqueara otro proyecto similar denominado *Cyber Intelligence Sharing and Protection Act* o CISPA. El objetivo que persiguen ambos proyectos es el de incentivar la monitorización y la detección de peligros informáticos en tiempo real. Para ello, se quiere crear una comunidad de ciberinteligencia, en la que se comparta la información recogida durante estos controles y supervisiones, tanto por el gobierno como por empresas privadas[1500]. Pese a que se contempla la protección de los derechos de los ciudadanos, esta protección no puede equipararse a la contemplada por las leyes europeas[1501].

Por otro lado, también se puede apreciar mayor sensibilidad, incluso de empresas estadounidenses, ante la necesidad de proteger los datos de sus clientes europeos, sin duda ante el temor de una reacción del mercado a favor de proveedores más respetuosos con los derechos[1502].

[1500] De esta forma se autoriza que estas empresas privadas monitoricen sus sistemas y los de sus clientes (si bien con su consentimiento) y que compartan la información obtenida con el gobierno (*Section 4*). Se establece la exclusión de responsabilidad en los casos en los que se cumpla con lo establecido en la ley respecto a la monitorización y el hecho de compartir la información (*Section 6*). *S.2588 Cybersecurity Information Sharing Act of 2014, 113th congress (2013-2014)* 10.7.2014, https://www.congress.gov/bill/113th-congress/senate-bill/2588/text, G. S. MCNEAL, "*Controversial cybersecurity bill known as CISA advances out of Senate Committee*", *Forbes Business*, 9.7.2014, http://www.forbes.com/sites/gregorymcneal/2014/07/09/controversial-cybersecurity-bill-known-as-cisa-advances-out-of-senate-committee/, (fecha consultas: 30.11.2014).

[1501] Si bien se contempla la posibilidad de que las empresas extraigan los datos personales, la regulación es tibia, ya que lo establece como algo que debe valorar la empresa (*Section 4*). También contempla la adopción por el Fiscal General (*Attorney General*) de una guía para asegurar el respeto de la privacidad y las libertades civiles de los ciudadanos en la recepción, conservación, uso y comunicación de la información de ciberseguridad. Por tanto, queda en manos del Fiscal el establecimiento de estas pautas (*Section 5*). *S.2588 Cybersecurity Information Sharing Act of 2014, 113th congress (2013-2014)* 10.7.2014, *op. cit.*.

[1502] EL 29 de abril de 2014 el periódico *theguardian.com* publicaba la noticia de que un juez estadounidense de Nueva York había ordenado que *Microsoft* le facilitara, en virtud de una orden de registro (*search warrant)*, la información personal que incluía los correos electrónicos personales de un usuario, aunque esta información se hallara en servidores ubicados fuera del territorio de los Estados Unidos, en concreto estaban en los servidores de *Microsoft* ubicados en Dublín, Irlanda. En esta sentencia, el juez argumentaba

El GA29 estima necesario introducir la protección en instrumentos internacionales, de forma que se asegure el respeto, en todos los niveles y en todos los países del globo, de los datos personales. Así, el grupo menciona, en concreto, la posibilidad de adoptar un protocolo adicional al artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de la ONU, como posible vía para adoptar unos principios de protección de datos, al estilo de la Propuesta de Madrid[1503]. Y es que por mucho que en Europa se protejan los derechos, queda demostrado que la protección debe producirse a nivel global, como global es Internet y el intercambio de información. En este sentido, la designación del relator especial sobre el derecho a la privacidad, por el Consejo de Derechos Humanos de Naciones Unidas es, sin duda, una noticia positiva.

Pero mientras se trabaja en la adopción de normas internacionales, o en la negociación con EEUU a nivel político, de momento son los responsables quienes deben negarse a proporcionar los datos, si no ven claro que, en nombre de la proporcionalidad, esto pueda considerarse necesario y deben realizar una interpretación estricta de lo que se considere dentro de la excepción de seguridad nacional[1504]. En definitiva, son los responsables, quienes deben realizar esta valoración.

---

que la orden se ejecutaba como una *subpoena* de solicitud de información al proveedor de servicios que poseía la información para que fuera el encargado de obtener la información y proporcionarla. Y es que *Microsoft* se defendía con el argumento de que que si el gobierno, en virtud de una orden de registro no podía acceder a un domicilio que radicara en el extranjero tampoco debería poder acceder a la información electrónica. *Microsoft* anunciaba su intención de llegar hasta el final del procedimiento judicial para defender sus compromisos con la protección de la privacidad de sus clientes y conseguir que mediante un pronunciamiento judicial se corrigiera esta postura del gobierno. S. GIBBS, "*US court forces Microsoft to hand over personal data from Irish server*", *The guardian*, 29.4.2014, http://www.theguardian.com/technology/2014/apr/29/us-court-microsoft-personal-data-emails-irish-server y D. HOWARD, *Corporate Vice President & Deputy General Counsel, Microsoft, "One step on the path to challenging search warrant jurisdiction", Microsoft on the Issues*, 25.4.2014, http://blogs.microsoft.com/on-the-issues/2014/04/25/one-step-on-the-path-to-challenging-search-warrant-jurisdiction/, (fecha consultas: 29.11.2014).

[1503] *Opinion 4/2014 on surveillance of electronic communications for intelligence and national security purposes, op. cit.*, pág. 16.

[1504] Si bien el GA29 reconoce que la solución debe adoptarse a nivel político, recalca que no debe excluirse la posibilidad de ir en contra de las empresas responsables que, de manera consciente, hayan colaborado con servicios de inteligencia de forma que les hayan permitido acceder a sus datos. Asimismo propugna una mayor transparencia por parte de estas empresas de cara a informar a los interesados sobre estas comunicaciones de datos. *Opinion 4/2014 on surveillance of electronic communications for intelligence and national security purposes, op. cit.*, págs. 7 a 8.

3.3. La insuficiencia de la figura: la responsabilidad de la tecnología

La Directiva 95/46/CE, pese a haberse aprobado con anterioridad a la aparición de todas estas tecnologías, incluye en su Considerando 46, la mención de que la adopción de las medidas de seguridad debe realizarse "tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos, sobre todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado". Este Considerando resalta la importancia de que la seguridad debe incorporarse desde el momento de la concepción del sistema de tratamiento.

Como se comentó en este trabajo, desde la UE se ha tratado de incentivar el uso de tecnologías que favorecieran la protección de datos, mediante las *Privacy Enhancing Technologies* (PET), hasta lo que se conoce como protección de datos desde el diseño (*privacy by design*) [1505], o la protección de datos por defecto (*privacy by default*)[1506]. También se ha trabajado en la elaboración de estándares y certificaciones de productos y servicios tecnológicos, así como de profesionales expertos[1507].

Esta tendencia responde a la insuficiencia de la figura del responsable para poder cumplir efectivamente la normativa, cuando la tecnología que utiliza no permite que eso sea posible. El desarrollador del *software,* que servirá para tratar datos personales, no activará el rol de responsable, ni siquiera el de encargado del tratamiento (a no ser que prestara servicios de mantenimiento y tuviera acceso a los datos personales). Sin embargo, su labor es clave para que el responsable pueda cumplir la normativa. De hecho, algún autor ha sugerido la incorporación de la regulación en la tecnología, de forma que fuera el código informático el que regulara la conducta de los usuarios[1508]. En definitiva,

[1505] A. CAVOUKIAN, *Privacy by design… Take the challenge*, *op. cit.*.
[1506] Ver Capítulo V.
[1507] Hay que recordar los estándares elaborados por el CEN en materia de privacidad y los que se han impulsado para incorporar la *privacy by design* en los procesos de fabricación y desarrollo de equipos y programas informáticos. Asimismo, cabe recordar las certificaciones de productos y servicios tecnológicos impulsadas por algunos Estados miembros (Alemania, Francia o Liechtenstein) o por entidades apoyadas por la UE, como *Europrise*. Ver Capítulos V y VI. En el ámbito del *cloud computing*, también se señalaba la iniciativa en materia de certificaciones, que pretendía facilitar su uso.
[1508] LESSIG considera el ciberespacio que iría más allá de lo que es meramente Internet, de forma que se trataría de la comunidad que se ha creado, una sociedad digital. En el ciberespacio, este autor, considera que se puede modificar la conducta de las personas mediante diversas vías de regulación que vendrían de la ley, el mercado, las normas o usos sociales y de la propia arquitectura. La arquitectura del ciberespacio es lo que Lessig denomina el "código". El código serían las instrucciones contenidas en el *software* o en el *hardware*

lo que se persigue es que "si la tecnología es el problema, la tecnología sea la solución"[1509].

El responsable, al igual que sucedía con los servicios de *cloud computing*, debería analizar si ese producto de *software* le posibilitará cumplir con la normativa. En caso de que la respuesta fuera negativa no debería adquirirlo. No obstante, en ocasiones el responsable no tendrá la capacidad ni los recursos de realizar un análisis informático y ¿no sería más lógico que los productos de *software* permitieran el respeto de la legislación de protección de datos si su finalidad es tratar datos personales?

Y no sólo eso, sino que así se lucharía también contra la complejidad del entorno digital, en el que los modelos de negocio incluyen una gran cantidad de participantes y un elevado intercambio de datos entre los mismos que se realiza de forma automática. Esto dificulta sobremanera la asignación de responsabilidades entre los diversos participantes y obliga a analizar si nos hallamos ante casos de corresponsabilidad o en los que se contemplan relaciones de subordinación, con encargados del tratamiento. Si la misma tecnología pudiera garantizar la aplicación de los principios de la normativa de protección de datos, de forma automática, facilitaría su cumplimiento y contrarrestaría esos problemas de atribución de responsabilidades[1510].

Así, por ejemplo, en el modelo de negocio de *Internet of things* puede ser posible que el fabricante subcontrate a otros sujetos para que le proporcionen los componentes del objeto o que incluso diseñen toda la parte del *hardware*[1511]. Es bastante habitual que

---

que hacen que el ciberespacio sea como es. L. LESSIG, *Code, version 2.0*. Basic Books, USA, 2006, págs. 121 a 124, 138.

[1509] Esta cita (*"if the technology is the problema, the technology may be the answer"*) aparece en J.M. DINANT, C. DE TERWANGNE, J.P. MOINY, *Rapport sur les lacunes de la Convention nº 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques*, Le Bureau du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques (T-PD-BUR) T-PD-BUR(2010)09, CRID, pág. 11.

[1510] Según un informe del Foro Económico Mundial, las respuestas a las preguntas ¿quién tiene tus datos?, ¿dónde están ubicados esos datos? son imposibles actualmente, por lo que entiende que el reto de la responsabilidad (*accountability)* es saber qué principios deben aplicarse y cómo. La respuesta, concluye el informe, debe hallarse en la tecnología misma que tiene el potencial de ser parte de la solución para asegurar la *accountability* a través de los controles pertinentes. El principio de *Privacy by design* será clave para asegurar que la privacidad se encuentre embebida en la tecnología. *Unlocking the value of personal data: from collection to usage, World Economic Forum, op. cit.*, pág. 3.

[1511] *Opinion 8/2014 on the recent developments on the Internet of Things, 14/EN WP 223, 16.9.2014, Article 29 Data Protection Working Party*, pág. 18.

los sensores, que se incorporan en los objetos, los fabrique un tercero (por ejemplo, un fabricante de neveras comprará a un tercero los sensores que incorporará a la nevera). Asimismo, cualquier desarrollador puede comprar estos sensores para diseñar su propia aplicación y adaptarla a un objeto. Los fabricantes de estas piezas no se considerarán responsables, ya que no determinarán los medios y los fines del tratamiento. Sin embargo, estos sujetos tienen un papel importante porque si lo que fabrican no incluye, por ejemplo, las debidas medidas de seguridad, puede comportar que no se protejan debidamente los datos personales[1512].

Pues bien, los fabricantes deberían tener en cuenta que sus productos deberán contar con las medidas de seguridad pertinentes, para que luego los responsables puedan garantizar la protección de los derechos de sus usuarios. Como indicó la Comisión, si bien, desde un punto de vista jurídico, la responsabilidad del cumplimiento de la normativa es de los responsables, desde el punto de vista social y ético, también recae en parte, en quienes elaboran las especificaciones técnicas y desarrollan los programas o sistemas[1513].

Por eso, además de responsabilizar a la tecnología, en algún caso se ha buscado también a quién está detrás de esta tecnología. Así, se puede señalar la Ley alemana de protección de datos, que ha incorporado como sujetos obligados a los fabricantes y desarrolladores de dispositivos destinados al tratamiento de datos (art. 6.c Ley alemana)[1514]. La legislación española también quiso obligar a los fabricantes de *software* a informar sobre el nivel de medidas de seguridad que éste cumplía, sin mucho éxito[1515].

[1512] En este entorno es especialmente complicado que los objetos tengan un nivel adecuado de seguridad, ya que habitualmente se cuenta con recursos limitados en cuestión de alimentación y capacidad de procesamiento. Estos objetos suelen ser vulnerables a ataques y no se suelen realizar actualizaciones que reparen estas vulnerabilidades. *Ibídem*, págs. 18 a 19. Como ejemplo, el 20 de enero de 2014 se conocía la noticia de un primer ataque conocido a estos objetos interconectados, entre los que se encontraba una nevera, que formaba parte de una *botnet*, una red de equipos comprometidos que contaba con 100.000 dispositivos conectados cuya finalidad era la de enviar spam. "Un ciberataque desde el televisor… e incluso desde un frigorífico" *El Mundo AFP*, 20.1.2014, http://www.elmundo.es/tecnologia/2014/01/20/52dce799ca4741d2548b4571.html, (fecha consulta: 1.12.2014).

[1513] Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET), COM(2007) 228 final, Bruselas, 2.5.2007, pág.3.

[1514] Ver Capítulo V.

[1515] Se introdujo en la Disposición adicional única del RLOPD: "Productos de software. Los productos de software destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto, que permitan alcanzar de acuerdo con lo establecido en el título VIII de este reglamento". No obstante, esta disposición no ha tenido aplicación práctica entiendo

Ya durante la modificación de la Directiva 97/66/CE[1516], derogada por la vigente Directiva 2002/58/CE, el GA29 incidió en la importancia de que la industria informática trabajara en productos de Internet que respetaran la vida privada y que facilitaran los instrumentos necesarios para ajustarse a la normativa europea sobre protección de datos. Además animaba a que la revisión de la Directiva se aprovechara para volver a analizar las responsabilidades que correspondían a los operadores de la red y a los proveedores de servicios en el ámbito de las telecomunicaciones[1517]. En esta línea también hay que recordar que el grupo de expertos encargado de la reforma de la Guía OCDE 2013 dejó pendiente de abordar en el futuro si debían añadirse, en la regulación de protección de datos, otros sujetos obligados, además del responsable, como el del desarrollador de sistemas informáticos[1518].

Sin embargo, lo que se concluye es que será el responsable quien deberá asegurarse que la tecnología que utilice pueda cumplir con lo establecido en la normativa. Por tanto, debería incentivarse el desarrollo de productos y servicios que, tecnológicamente, permitan de una forma fácil la protección de los derechos de sus usuarios. En una sociedad tecnológica, la seguridad y la protección de las personas deben estar integradas en la tecnología y no depender, únicamente, de la elección del responsable, como solución.

---

que principalmente porque no acarrea ninguna sanción, al limitarse la responsabilidad al responsable y al encargado del tratamiento.

[1516] Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, DO L 24 de 30.1.1998.

[1517] Dictamen 2/2000 sobre la revisión general de la normativa de telecomunicaciones, 5009/00/ES/final WP 29, 3.2.2000, Grupo operativo sobre Internet, Grupo de trabajo Artículo 29 sobre la protección de datos, págs. 3 a 4.

[1518] OECD (2013), "*Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines*", *OECD Digital Economy Papers, No. 229, OECD Publishing*, pág. 11. http://dx.doi.org/10.1787/5k3xz5zmj2mx-en (fecha consulta: 8.8.2014).

CAPÍTULO IX

RESPUESTAS DEL LEGISLADOR ANTE LOS RETOS PLANTEADOS A LA FIGURA DEL RESPONSABLE

De las tensiones apuntadas en el capítulo anterior resulta patente que el derecho a la protección de datos está sometido a importantes retos que exigen un cambio en los instrumentos que hasta ahora se han utilizado para regularlo.

La importancia de este derecho, en la actualidad, se demuestra al haberse convertido la reforma emprendida por la UE, en enero de 2012, en epicentro de controversia y objeto de debate de alcance mundial.

En este capítulo me aproximaré a esta reforma de gran calado para ver cómo se ha incorporado la figura del responsable. También estimo interesante apuntar a otra reforma que se desarrolla paralelamente, la del Convenio 108, en el marco del Consejo de Europa, especialmente importante por dar cabida también a países no miembros. Por último, mencionaré un proyecto de ley que se tramita en EEUU: la *Consumer Privacy Bill of Rights Act*.

1. EL PROYECTO DE REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

1.1. El cambio de instrumento jurídico

En el año 2009 la Comisión Europea inició un examen de la legislación de la UE en materia de protección de datos, con el fin de detectar si ésta podía hacer frente al nuevo contexto tecnológico y social que se explicaba en el anterior capítulo[1519]. El resultado de esta revisión fue que los principios establecidos en la Directiva 95/46/CE seguían siendo válidos, pero se localizaron algunos problemas que exigían una solución. Así se señaló la necesidad de hacer frente al impacto de las nuevas tecnologías, a la

[1519] Se realizaron diversos estudios, una conferencia de alto nivel en mayo de 2009 y una consulta pública que duró hasta finales de 2009. Los resultados se reflejaron en la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, un enfoque global de la protección de los datos personales en la Unión Europea, *op. cit.*. Después se realizó otra consulta pública del 4 de noviembre de 2010 al 15 de enero de 2011 y también se llevaron a cabo consultas específicas, conferencias y se organizaron diversos actos con autoridades, operadores del sector privado y organizaciones de consumidores. PCE-RGPD, págs. 3 a 4.

insuficiente armonización de las legislaciones de los Estados miembros, a la globalización, al necesario refuerzo del papel de las autoridades de control y a la necesidad de mejorar la coherencia del marco jurídico, mediante un instrumento global aplicable a todas las operaciones de tratamiento de datos, en todos los sectores y políticas de la Unión[1520].

A estas necesidades se unió el reconocimiento del derecho a la protección de datos en el artículo 8 de la Carta UE[1521] y la instauración de una nueva base jurídica, el artículo 16 TFUE[1522]. Esto supuso un cambio importante en la orientación de la normativa, que ya no sólo perseguía una finalidad económica, que precisaba de forma indirecta de la protección de unos derechos, sino que ahora también perseguía sin ambages la protección de un derecho fundamental.

La adopción de estas nuevas disposiciones, además, se incardina en un nuevo panorama propiciado por el Tratado de Lisboa, que supuso la eliminación de la clásica separación entre los pilares, si bien es cierto que, en materia de protección de datos personales se mantiene una diferenciación entre los mismos[1523].

Finalmente, el 25 de enero de 2012, la Comisión Europea presentó la propuesta de un nuevo marco jurídico para la protección de los datos personales en la UE. Con esta

[1520] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, un enfoque global de la protección de los datos personales en la Unión Europea, *op. cit.*, págs. 3 a 4.

[1521] Ver Capítulo II.

[1522] El artículo 16 TFUE reconoce el derecho a la protección de datos de carácter personal y establece una base jurídica que permite al Parlamento Europeo y al Consejo adoptar normas en esta materia. Estas normas deben versar sobre la protección de las personas físicas respecto del tratamiento de datos que llevan a cabo las instituciones, órganos y organismos de la Unión y los que lleven a cabo los Estados miembros, en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión y sobre la libre circulación de los datos.

[1523] Esta estructura en pilares fue introducida por el Tratado de Maastricht de 1992. El primer pilar era el pilar comunitario, donde se incluían las cuestiones supranacionales y que correspondía a las tres comunidades (Comunidad Europea, Comunidad Europea de la Energía Atómica o Euratom y Comunidad Europea del Carbón y del Acero o CECA). El segundo pilar era el correspondiente a la política exterior y de seguridad común regulada en el título V del TUE. El tercer pilar era el correspondiente a la cooperación policial y judicial en materia penal, regulado en el título VI del TUE. En materia de protección de datos, además de la nueva base jurídica que representa el artículo 16 TFUE en esta materia, hay que tener en cuenta la Declaración nº 21 y el artículo 39 TUE. Estas disposiciones establecen que, respecto a la protección de datos, podrá ser necesario adoptar normas específicas en el ámbito de la cooperación judicial en materia penal y de cooperación policial y que en el ámbito de la política exterior y de seguridad común el Consejo adoptará una decisión específica. Por ello, se ha previsto la adopción de dos instrumentos diferenciados, uno de aplicación general a lo que sería la materia comunitaria y otro que se refiere a la cooperación judicial y policial.

propuesta se pretendía afrontar el impacto del desarrollo tecnológico acaecido desde la aprobación de la Directiva 95/46/CE y reflejaba el reconocimiento y la importancia del derecho a la protección de datos en el ordenamiento jurídico europeo[1524].

Este nuevo marco jurídico constaba de dos propuestas legislativas: un proyecto de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos) (PCE-RGPD)[1525], que sustituiría la vigente Directiva 95/46/CE, y un proyecto de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos (PCE-Directiva policía)[1526], que sustituiría a la actual Decisión marco 2008/977/JAI sobre esta materia.

Respecto al Reglamento General de Protección de Datos, el Parlamento Europeo, tras un largo proceso de elaboración, aprobó la Resolución legislativa, en primera lectura, el 12 de marzo de 2014 (PPE-RGPD)[1527]. El Consejo UE adoptó una orientación general

[1524] Como reflejó el discurso de presentación de la reforma por Viviane Reding, en aquel entonces Comisaria de Justicia de la UE y Vicepresidenta de la Comisión: «Hace 17 años, menos de un 1 % de los europeos usaba Internet. Hoy en día se transfieren e intercambian enormes cantidades de datos personales entre continentes y de una punta a otra del mundo en fracciones de segundos» (…)«La protección de los datos personales es un derecho fundamental de todos los europeos, quienes, no obstante, a veces sienten que pierden el control sobre sus datos personales. Mis propuestas contribuirán a infundir confianza en los servicios en línea dado que los ciudadanos estarán mejor informados de sus derechos y tendrán un mayor control sobre la información que les atañe. La reforma conseguirá todos estos objetivos al tiempo que facilitará el funcionamiento de las empresas y les permitirá ahorrar costes. La existencia de un marco legal sólido, claro y uniforme a escala de la UE permitirá liberar el potencial del Mercado Único Digital y fomentar el crecimiento económico, la innovación y la creación de empleo». Comunicado de prensa de Bruselas, 25.1.2012. http://europa.eu/rapid/press-release_IP-12-46_es.htm, (fecha consulta: 3.12.2014).

[1525] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), COM(2012)11final 2012/0010 (COD), Bruselas, 25.1.2012 (PCE-RGPD).

[1526] Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, COM(2012)10 final 2012/0010 (COD), Bruselas, 25.1.2012 (PCE-Directiva policía).

[1527] Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), P7_TA-PROV(2014)0212.

del texto, el 15 de junio de 2015 (PCJ-RGPD)[1528]. El 24 de junio de 2015 se iniciaron los diálogos tripartitos entre Comisión, Parlamento y Consejo, con el fin de llegar a un acuerdo que se espera sea a finales de 2015. El Consejo UE puede adoptar el texto del Parlamento o adoptar el texto negociado, en primera lectura que el Parlamento debería aprobar en segunda lectura, en lo que se conoce como acuerdo temprano en segunda lectura (art. 294 TFUE). Por esta razón, hay que realizar una aproximación a los tres textos, ya que no podemos saber cuál será la regulación final.

La Comisión, en su propuesta, tras evaluar diferentes opciones para afrontar esta reforma legislativa, decidió optar por elevar el nivel de armonización mediante el uso de instrumentos jurídicos más sólidos. Por ello, se decidió sustituir la Directiva 95/46/CE por un reglamento y la decisión marco por una directiva, considerándose ambos instrumentos más adecuados para dar respuesta a los objetivos planteados[1529].

Si centramos el análisis en el reglamento cabe plantearse ¿qué implicaciones tiene el que ahora se apruebe un reglamento y no una directiva? El reglamento es la norma por excelencia de la UE, tiene alcance general, es obligatorio en todos sus elementos y directamente aplicable en los Estados miembros (art. 288 TFUE). Por tanto, es una norma que crea derechos y obligaciones para sus destinatarios, sin necesidad de que se adapte o transponga por normas de los Estados miembros.

[1528] Nota de la Presidencia al Consejo sobre Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)-Preparación de un planteamiento general, Expediente interinstitucional: 2012/2011 (COD) 9565/15, Bruselas, 11.6.2015.

[1529] La Comisión barajó tres opciones legislativas: la primera, introducir enmiendas legislativas mínimas y el uso de comunicaciones interpretativas y medidas de apoyo estratégico; la segunda, un paquete de disposiciones legislativas que abordaran cada una las diferentes cuestiones identificadas; la tercera, la centralización de la protección de datos, mediante normas precisas y detalladas para todos los sectores y la creación de una agencia de la UE para supervisar y ejecutar las disposiciones. Después del análisis de impacto de todas las opciones, se optó por una solución híbrida, que se decantaba por la segunda opción, con algunos elementos de las otras dos. Según la evaluación de impacto realizada, con esta opción se conseguiría una mayor seguridad jurídica para responsables del tratamiento y ciudadanos, reducir la carga administrativa, coherencia en la aplicación en la Unión, la posibilidad efectiva de que las personas físicas ejercieran sus derechos y la eficiencia en la supervisión y control. PCE-RGPD, págs. 5 a 6, según los resultados del estudio de impacto que se incluye en el documento *Commission Staff Working Paper, Impact assessment accompanying the document Regulation of the European Parliament […], op. cit.*. El Supervisor Europeo de Protección de Datos también había sugerido que fuera un reglamento el instrumento utilizado para sustituir la Directiva 95/46/CE y así lograr una mayor armonización. Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones — «Un enfoque global de la protección de los datos personales en la Unión Europea» (2011/C 181/01) 22.6.2011, pág. 9.

Alrededor de la elección del reglamento como instrumento jurídico que sustituirá la Directiva 95/46/CE quiero destacar tres cuestiones: los principios de subsidiaridad y proporcionalidad, la limitación del ámbito de aplicación de la base jurídica utilizada y las dudas suscitadas sobre el respeto del sistema de derechos fundamentales nacional.

1.1.1. Los principios de subsidiaridad y proporcionalidad

Al versar el reglamento sobre una competencia, que entiendo no es exclusiva de la UE[1530], entra en juego el principio de subsidiaridad. En virtud de este principio, "la Unión intervendrá sólo en caso de que, y en la medida en que, los objetivos de la acción pretendida no puedan ser alcanzados de manera suficiente por los Estados miembros, ni a nivel central ni a nivel regional y local, sino que puedan alcanzarse mejor, debido a la dimensión o a los efectos de la acción pretendida, a escala de la Unión" (art. 5.3 TUE).

También debe respetarse el principio de proporcionalidad, de forma que el contenido y la forma de la acción no deben exceder de lo necesario para alcanzar los objetivos. Pese a que la Comisión considera, que en sus propuestas, se respetan los principios de subsidiaridad y proporcionalidad, no todos los Estados miembros están de acuerdo.

Ambos principios cuentan con un mecanismo que permite el control por parte de los Parlamentos nacionales de los Estados miembros, el conocido como mecanismo de "alerta temprana", que se encuentra en el Protocolo nº 2 sobre la aplicación de los principios de subsidiaridad y proporcionalidad[1531]. De acuerdo con este protocolo, los Parlamentos de los Estados miembros pueden presentar un dictamen motivado si consideran que no se respetan estos principios. En caso de que los dictámenes presentados por los Parlamentos representaran un tercio de los votos que se atribuyen mediante el artículo 7 del protocolo (dos votos por cada Parlamento nacional), debería volverse a estudiar el proyecto de acto legislativo.

[1530] El artículo 4 TFUE establece que "1. La Unión dispondrá de competencia compartida con los Estados miembros cuando los Tratados le atribuyan una competencia que no corresponda a los ámbitos mencionados en los artículos 3 y 6", en los que no puede encajarse la materia a la que se refiere el reglamento.

[1531] Protocolo nº 2 sobre la aplicación de los principios de subsidiaridad y proporcionalidad, Versiones consolidadas del Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea, DO 2010/C 83/206 de 30.3.2010.

Algunos Parlamentos nacionales presentaron dictámenes en los que concluían que no se respetaba el principio de subsidiaridad al utilizarse un reglamento en vez de una directiva. En concreto, los dictámenes presentados fueron los de la Cámara de Representantes belga, el *Bundesrat* alemán[1532], el Senado francés, la Cámara de Diputados italiana y el Parlamento sueco, por lo que no se alcanzó el *quórum* que obligaría a revisar la propuesta. En consecuencia, hay que entender que se respeta el principio de subsidiaridad. La UE está en mejores condiciones que los Estados miembros para garantizar una protección uniforme del derecho a la protección de datos de los ciudadanos europeos[1533].

1.1.2. La limitación de la base jurídica que introduce el artículo 16.2 TFUE

El artículo 16.2 TFUE, al referirse a los tratamientos de datos sobre los que podrá versar la norma que se adopte en virtud del mismo, indica que serán los que lleven a cabo los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión y sobre la libre circulación de los datos.

En virtud de esta limitación se plantea la cuestión relativa a ¿qué sucederá en el caso de que nos hallemos ante un supuesto que no entre dentro del ámbito de aplicación del Derecho de la Unión o que no afecte a la libre circulación de los datos? ¿Deberán mantenerse las leyes nacionales de protección de datos actuales para estos supuestos? ¿Cómo diferenciarán los operadores cuando estamos ante un supuesto u otro?[1534]

[1532] Entre otras cuestiones, el *Bundesrat* alemán indicaba en su dictamen que no se demostraba suficientemente la necesidad de elegir un reglamento que además se aplicaría tanto al sector privado, como al público, de forma que desplazaría las normativas de los Estados miembros cuando en algunos de estos países, como sucedía en Alemania, ya había suficientes garantías directamente aplicables y que ofrecían un alto grado de seguridad jurídica. Así el parlamento alemán entendía que la primacía del reglamento pondría en jaque la existencia de áreas nucleares de la legislación de protección de datos alemana como la de los tratamientos de la seguridad social o la videovigilancia. *Decision of the Bundesrat 52/12 30.3.2012 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012)11 FINAL; Council document 5853/12*, http://www.bundesrat.de/SharedDocs/downloads/EN/uebersetzungen/0052-12b-en.pdf;jsessionid=EF0BF5125BC4D2C5B8BA3C1018DFB362.2_cid374?__blob=publicationFile&v=1, (fecha consulta: 5.12.2014).

[1533] A. RALLO LOMBARTE, "Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma", *UNED, Revista de derecho político*, *op. cit.*, pág. 30.

[1534] R. MARTÍNEZ MARTÍNEZ, "El complejo encaje normativo de la propuesta de Reglamento general de protección de Datos de la Unión Europea", *Actualidad jurídica Aranzadi*, nº 839, 2012, pág. 3.

Si bien, en la teoría esta cuestión podría parecer enormemente relevante, en definitiva, estimo que no aporta grandes diferencias respecto a la regulación ya existente en la Directiva 95/46/CE. En primer lugar, porque la misma Directiva 95/46/CE ya contenía también estas limitaciones. En el asunto *Lindqvist* se plantearon estas cuestiones respecto a la Directiva 95/46/CE con la base jurídica en la que se apoyaba. El TJUE entendió que no debía darse a la expresión "actividades no comprendidas en el ámbito de aplicación del Derecho comunitario" un alcance que implicara comprobar caso por caso si la actividad concreta afectaba directamente a la libre circulación entre los Estados miembros[1535].

En ese mismo sentido, el TJUE interpretó que las actividades, que en el artículo 3.2 Directiva 95/46/CE se citan como ejemplos de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, tienen por objeto delimitar el alcance de la excepción que se establece en esta disposición, de modo que sólo se aplique a aquellas actividades que se mencionan expresamente o que pueden incluirse en la misma categoría (*eiusdem generis*)[1536].

En definitiva, en función de esta jurisprudencia, los supuestos en los que cabría entender que no debe aplicarse el derecho europeo en el marco de la Directiva 95/46/CE deben interpretarse restrictivamente. La normativa nacional que haya transpuesto la Directiva 95/46/CE y haya seguido las limitaciones de su ámbito de aplicación será normativa que sólo se aplicará cuando se esté dentro del ámbito de aplicación del Derecho de la Unión o cuando se afecte la libertad de circulación de los datos. Por tanto, no debería darse el conflicto entre esta normativa y el futuro reglamento adoptado en

[1535] La señora *Lindqvist* alegaba que su conducta como particular, consistente en crear una página web en su tiempo libre y publicar en ella información en ejercicio de su derecho a la libertad de expresión, no estaba sujeta al derecho comunitario, ya que no había realizado ninguna actividad económica. Por tanto, no se le podía aplicar la directiva porque eso implicaría que el legislador se habría excedido en las competencias que, en aquel entonces artículo 100 A del Tratado CE, le atribuían. El TJUE interpretó que el hecho de acudir a la base jurídica del artículo 100 A del Tratado CE no presuponía la existencia de un vínculo efectivo con la libre circulación entre Estados miembros en cada una de las situaciones comprendidas por el acto que se funda en tal base, es decir, la Directiva 95/46/CE en el caso analizado. Si se interpretara lo contrario, el TJUE opinó que podría hacer que los límites de la directiva se volvieran inciertos y aleatorios, lo que sería contrario al objetivo de ésta que era la aproximación de normativas para eliminar obstáculos al funcionamiento del mercado interior. Sentencia del TJUE de 6 de noviembre de 2003, *Bodil Lindqvist*, C-101/01, EU:C:2003:596, apdos. 40-42 (ver también Sentencia del TJUE de 20 de mayo de 2003, *Rechnungshof/Österreichischer Rundfunk* y otros C-465/00, C-138/01 y C-139/01, EU:C:2003:294, apdos. 41-42).

[1536] Sentencia del TJUE de 6 de noviembre de 2003, *Bodil Lindqvist*, C-101/01, EU:C:2003:596, apdo. 44.

virtud del artículo 16.2 TFUE. Ahora bien, en aquellos ordenamientos en los que las leyes nacionales se apliquen a supuestos fuera del ámbito de aplicación del Derecho de la Unión o que no afecten a la libertad de circulación, sí podrá darse el conflicto.

Por otro lado, al versar sobre una competencia compartida entre la Unión y los Estados miembros, el reglamento no necesariamente debe unificar el ordenamiento de los Estados miembros[1537]. Sin embargo, entiendo que desde el momento en el que la Unión ha optado por ejercer su competencia, los Estados ya no podrán ejercerla a partir de ese momento ni, por tanto, legislar[1538]. Y bien sea porque unifique el ordenamiento y, por tanto, desplace automáticamente todas las normas, sea cual fuera su rango, del orden interno de los Estados miembros que versen sobre la materia o porque se proceda a la inaplicación de las normas que contradigan lo que disponga el reglamento, el resultado será la práctica ineficacia de las regulaciones nacionales en la materia, fuera de los casos apuntados que queden fuera del ámbito de aplicación del Derecho de la Unión o que no afectaran a la libre circulación de los datos.

Ahora bien, el texto adoptado por el Consejo UE introduce algunas disposiciones, con el fin de matizar y aclarar el alcance del desplazamiento de la legislación nacional. Y es que, sin perjuicio de lo indicado, hay que decir que, en el texto del reglamento, se encuentran algunas vías que remiten a las legislaciones nacionales, como los supuestos que permitirán la legitimación, que podrán hallarse en las disposiciones nacionales[1539].

En ningún caso los responsables pueden limitarse al conocimiento del reglamento, sino que lo deberán encuadrar en las normativas sectoriales aplicables. Sin embargo, merece algunas dudas el hecho de que se permita, en el texto del Consejo UE, que las

[1537] E. LINDE PANIAGUA, "Capítulo IV. El sistema de fuentes del derecho de la Unión Europea", E. LINDE PANIAGUA, M. BACIGALUPO SAGGESE, J.A. FUENTETAJA PASTOR. *Principios de Derecho de la Unión Europeo*, 4ª Ed., Constitución y Leyes, Madrid, 2011, pág. 369.

[1538] Así lo establece el artículo 2.2 TFUE que indica que "Cuando los Tratados atribuyan a la Unión una competencia compartida con los Estados miembros en un ámbito determinado, la Unión y los Estados miembros podrán legislar y adoptar actos jurídicamente vinculantes en dicho ámbito. Los Estados miembros ejercerán su competencia en la medida en que la Unión no haya ejercido la suya. Los Estados miembros ejercerán de nuevo su competencia en la medida en que la Unión haya decidido dejar de ejercer la suya."

[1539] Se pueden citar las remisiones a las leyes nacionales para servir de base jurídica del tratamiento de los datos (artículo 6.1, apartados d) y e) PCE-RGPD) o las habilitaciones a los Estados miembros para legislar contenidas en el capítulo IX sobre disposiciones relativas a situaciones de tratamiento de datos específicas. Se trata de habilitaciones para legislar sobre tratamientos de ámbito sectorial pero que se deberán ajustar a los límites que establece el mismo reglamento. Así también lo indica la *Opinion of the European Data Protection Supervisor on the data protection reform package,* 7.3.2012, págs 9 a 12.

normas nacionales sectoriales promulgadas para aplicar la Directiva 95/46/CE se mantengan. Entiendo que se podrán mantener siempre que respeten la regulación del reglamento[1540].

1.1.3. Las dudas sobre el respeto del sistema de derechos fundamentales nacional

Otra cuestión suscitada, esta vez más débilmente, ha sido el hecho de si el reglamento puede versar sobre una materia, como es un derecho fundamental, que afecta al núcleo de los ordenamientos jurídicos de los Estados miembros[1541]. Si bien en nuestro país cabe la posibilidad de que pudieran plantearse, en el futuro, conflictos a este respecto será en supuestos concretos, en los que pudiera llegar a entrar a valorar el Tribunal Constitucional[1542]. No obstante, parece difícil vislumbrar una situación de conflicto, cuando el reglamento ha estado sometido a un proceso largo de debate y ni siquiera se ha cuestionado por el Parlamento español que atente contra el principio de subsidiaridad[1543].

[1540] A esta previsión de la parte del preámbulo, el texto del Consejo UE añade otra previsión bastante ambigua sobre la posibilidad que se brinda a los Estados miembros de incorporar la regulación del Reglamento a sus legislaciones, en los casos en que éste establezca especificaciones o restricciones de sus normas por la legislación nacional (art. 1.2bis, Considerandos 6bis y 8 PCJ-RGPD). Estas disposiciones no hacen sino aumentar la confusión entorno a una cuestión ya de por sí compleja.

[1541] R. MARTÍNEZ MARTÍNEZ, "El complejo encaje normativo de la propuesta de Reglamento general de protección de Datos de la Unión Europea", *Actualidad jurídica Aranzadi, op. cit.*, pág. 3. Así lo señalaba la Cámara de Diputados italiana en su *Reasoned opinion, Proposal for a regulation of the European Parliament and of the Council on the protección of individuals with regard to the processing of personal data and on the free movement of such data (COM(2012)11 Final).* LÓPEZ AGUILAR destacó precisamente que la aprobación de este paquete legislativo expresaba la dimension constitucional del Tratado de Lisboa. Como indicaba este autor, expresidente de la Comisión de Libertades, Justicia e Interior (Comisión LIBE) del Parlamento Europeo, que tramitó la propuesta, esta dimensión se manifiesta en el impacto del Reglamento que implicará el desplazamiento de una Ley Orgánica española. J.F. LÓPEZ AGUILAR, "Data protection package y Parlamento europeo", A. RALLO LOMBARTE, R. GARCÍA MAHAMUT (Ed.), VVAA, *Hacia un nuevo derecho europeo de protección de datos. Towards a new European data protection regime*, *op. cit.*, pág. 31.

[1542] Si bien el Tribunal Constitucional, al examinar la compatibilidad de la Carta UE incluida en la fallida constitución europea, no vió contradicciones con la Constitución Española, indicó que no podía pronunciarse respecto a los concretos problemas de articulación de los derechos que deberían suscitarse en el marco de los procedimientos que se le presenten. Y es que interpreta el Tribunal que "la cesión constitucional que el art. 93 CE posibilita tiene a su vez límites materiales que se imponen a la propia cesión. Esos límites materiales, no recogidos expresamente en el precepto constitucional, pero que implícitamente se derivan de la Constitución y del sentido esencial del propio precepto, se traducen en el respeto de la soberanía del Estado, de nuestras estructuras constitucionales básicas y del sistema valores y principios fundamentales consagrados en nuestra Constitución, en el que los derechos fundamentales adquieren sustantividad propia (art. 10.1 CE), límites que, como veremos después, se respetan escrupulosamente en el Tratado objeto de nuestro análisis." Declaración del Pleno del Tribunal Constitucional 1/2004, de 13 de diciembre de 2004. Requerimiento 6603-2004. Formulado por el Gobierno de la Nación, acerca de la constitucionalidad de los artículos I-6, II-111 y II-112 del Tratado por el que se establece una Constitución para Europa, firmado en Roma el 29 de octubre de 2004. (BOE núm. 3 Suplemento, de 4.1.2005), págs. 9 y 12.

[1543] Desde la adhesión a las Comunidades Europeas y en todas las reformas de los Tratados constitutivos, incluida la última de del Tratado de Lisboa, han sido aprobadas por el gobierno pero mediante ley orgánica.

Hay que indicar que, en el trámite parlamentario, se introdujo un precepto (art. 85bis PPE-RGPD), que precisamente incidía en el respeto de los derechos fundamentales, de forma que se afirmaba que el reglamento no podría tener por efecto una modificación de la obligación de respetar los derechos fundamentales y los principios jurídicos fundamentales consagrados en el artículo 6 del TUE.

1.2. El difícil camino a recorrer y la fragilidad de la voluntad legislativa ante el contexto político y social

Una señal indudable de la importancia de esta reforma es que no se han podido cumplir los calendarios previstos, ya que su adopción ha suscitado gran controversia y debate. El trámite parlamentario ha incluido más de cuatro mil enmiendas y se han producido presiones desde los sectores empresariales más afectados. No se recuerdan muchas más iniciativas legislativas europeas que hayan suscitado una presión similar por parte de los *lobbies*[1544]. En definitiva, las propuestas debían haberse aprobado antes de la celebración de las elecciones europeas en mayo de 2014, y sin embargo, esto no se logró.

Antes de que se presentara la reforma, el 25 de enero de 2012, algunos medios de comunicación se hicieron eco de las presiones protagonizadas por instituciones y empresas estadounidenses[1545]. En unas cartas informales enviadas por la *Federal Trade Commission* y por la embajada de EEUU se indicaban algunos puntos de la reforma sobre los que se realizaron recomendaciones[1546]. Asimismo, como muestra de las presiones se

---

Así la reforma de Lisboa ha sido aprobada por Ley Orgánica 1/2008, de 30 de julio, por la que se autoriza la ratificación por España del Tratado de Lisboa, por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea, firmado en la capital portuguesa el 13 de diciembre de 2007. C. GUTIÉRREZ ESPADA, M.J. CEVELL HORTAL, J.J. PIERNAS LÓPEZ, R. GARCIANDÍA GARMENDIA, *La Unión Europea y su derecho*, Trotta, Madrid, 2012, pág. 223.

[1544] J.F. LÓPEZ AGUILAR, "Data protection package y Parlamento europeo", A. RALLO LOMBARTE, R. GARCÍA MAHAMUT (Ed.), VVAA, *Hacia un nuevo derecho europeo de protección de datos. Towards a new European data protection regime*, *op. cit.*, pág. 31.

[1545] El 21 de julio de 2013 el diario El País publicaba una noticia de L. ABELLÁN titulada "EEUU presiona en la sombra para frenar la normativa de privacidad europea", en la que incluía dos misivas, una carta de la Comisión Federal de Comercio de diciembre de 2011 y una nota de la Embajada de EEUU de enero de 2012. http://internacional.elpais.com/internacional/2013/07/21/actualidad/1374420934_701911.html, (fecha consulta: 20.7.2013).

[1546] *Informal note on draft EU General Data Protection Regulation (december 2011). http://ep00.epimg.net/descargables/2013/07/21/d9d751c9b66cad403d4d2903c993cc63.pdf* (fecha consulta: 20.7.2013) *y Informal comment on the draft General Data Protection Regulation and draft Directive on Data Protection in Law Enforcement Investigations. http://ep00.epimg.net/descargables/2013/07/21/849c9e0486f3300b007ba7cd1c9b6412.pdf* (fecha consulta:

puede mencionar la publicación por una organización privada de algunas enmiendas que entidades de gran relevancia sugirieron a los eurodiputados[1547]. Esta organización comparó estas sugerencias con las enmiendas que finalmente presentaron los eurodiputados y halló hasta doscientas coincidencias.

Citaré dos de estas modificaciones por su relación con los temas expuestos en el anterior capítulo: la regulación del denominado derecho al olvido y las comunicaciones de datos no autorizadas por la legislación de la UE. Si se compara el borrador que se filtró, datado a finales de 2011 (PCE-RGPD no oficial)[1548], con la propuesta presentada el 25 de enero de 2012 (PCE-RGPD) y se completa el análisis con el texto resultante (PPE-RGPD), una vez realizada la primera lectura parlamentaria, se pueden extraer algunas conclusiones interesantes con relación a la eficacia de estas presiones.

Las instituciones estadounidenses fueron especialmente críticas con el artículo 42 PCE-RGPD no oficial. Este artículo obligaba al responsable del tratamiento o al encargado del tratamiento a solicitar autorización a la autoridad de control, cuando un tribunal o una autoridad administrativa de un tercer país les solicitaran la comunicación de datos personales[1549]. En las cartas mencionadas, se indicaba que este precepto obstaculizaría la acción de las autoridades estadounidenses en protección de intereses públicos e incluso la cooperación con entidades europeas. En la segunda carta se citan algunos convenios de colaboración, especialmente en materia financiera. Además, se

---

20.7.2013).

[1547] El proyecto citado por el artículo de El País es la página web *Lobbyplag* (www.lobbyplag.eu). Entre las entidades que sugirieron estas enmiendas cita a *Amazon*, *Facebook*, *Microsoft*, la Federación Europea de Banca y Telefónica. Además se comentan las afirmaciones del ponente en el Parlamento, Jan Philipp Albrecht sobre sus entrevistas con unas doscientas personas, durante el año anterior, especialmente con empresas, despachos de abogados y otros representantes.

[1548] *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), draft, Version 56 29.11.2011*, http://www.statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf, (fecha consulta: 8.12.2014).

[1549] En concreto el artículo 42.2 PCE-RGPD no oficial rezaba así: "*Where a judgment of a court or tribunal or a decision of an administrative authority of a third country requests a controller or processor to disclose personal data, the controller or processor and, if any, the controller's representative, shall notify the supervisory authority of the request without undue delay and must obtain prior authorisation for the transfer by the supervisory authority in accordance with point (b) of Article 31(1).*" En el memorándum explicativo, se fundamentaba la inclusión del artículo 42 en la prohibición, de acuerdo con la legislación europea, de que un responsable comunique datos personales a un país tercero, en estos casos, a no ser que estuviera autorizado por un convenio internacional o por una autoridad supervisora. A modo de ejemplo, se citaba el Reglamento (CE) nº 2271/96 del Consejo de 22 de noviembre de 1996 relativo a la protección contra los efectos de la aplicación extraterritorial de la legislación adoptada por un tercer país, y contra las acciones basadas en ella o derivadas de ella, DO L 309, 29.11.1996.

dificultaría también la fase de *discovery*, al ser las autoridades de protección de datos las que decidirían sobre la pertinencia de proporcionar las evidencias solicitadas en las investigaciones.

Pues bien, esta disposición se eliminó de la propuesta de la Comisión (PCE-RGPD). No obstante, se volvió a introducir en el trámite parlamentario, esta vez en un nuevo artículo 43 bis PPE-RGPD[1550]. Si se atiende al contexto social existente durante la tramitación de esta reforma, tal como se describía en el capítulo anterior, resulta elocuente. Inicialmente se respondió a las presiones del gobierno estadounidense. Sin embargo, tras desvelarse el alcance de los programas de espionaje y, por tanto, al elevarse la alarma social, durante el trámite parlamentario se volvieron a incluir las previsiones que se habían adoptado inicialmente. Este precepto no ha sido incorporado en la orientación del Consejo UE.

En lo que respecta a la regulación del derecho al olvido, ésta se diluyó en los textos de la Comisión y el Parlamento. Sin embargo, fue el TJUE el que consolidó, si no un derecho específico al olvido, sí un derecho de oposición y cancelación acorde con el objetivo que se perseguía con esa regulación inicial criticada en las mencionadas cartas[1551]. Pese a que el TJUE reconoció el derecho pero lo recondujo a los derechos regulados en la Directiva 95/46/CE, entiendo que favoreció que el Consejo UE volviera a incluir una referencia expresa a este derecho al olvido (art. 17 PCJ-RGPD).

1.3. El proyecto de Reglamento General de Protección de Datos

Con el fin de centrar el análisis que realizaré en los próximos apartados, hay que tener en cuenta que éste girará, principalmente, en torno a la propuesta presentada por la Comisión Europea (PCE-RGPD) que se completará con las modificaciones introducidas por la resolución del Parlamento (PPE-RGPD) y la orientación general del Consejo UE (PCJ-

[1550]Así, el artículo 43 bis.2 PCE-RGPD establece: "Si una sentencia de un tribunal o una decisión de una autoridad administrativa de un tercer país exigen a un responsable o encargado del tratamiento que haga públicos datos personales, el responsable o encargado del tratamiento y el representante del responsable del tratamiento, si lo hay, comunicarán a la autoridad de control competente la solicitud sin demoras injustificadas y deberán obtener la autorización previa para la transferencia o divulgación por la autoridad de control."

[1551] Ver CAP V.

RGPD)[1552]. Ambos textos del Parlamento y del Consejo UE lo que hacen es modificar la propuesta de la Comisión.

Nos hallamos, por tanto, ante una norma en trámite de elaboración y que tiene gran importancia, ya que se aplicará a los 28 Estados miembros de forma directa. El hecho de abordar un texto en fase de elaboración siempre es una tarea arriesgada, máxime cuando reviste complejidad, como es el caso. Sin embargo, he estimado imprescindible incluir la referencia a este proyecto que constituye, por el momento, el futuro inmediato de la figura del responsable en la UE.

La PCE-RGPD incluye once capítulos y, a primera vista, se puede observar la extensión del texto que duplica el de la Directiva 95/46/CE[1553]. El Capítulo I contiene las disposiciones generales, que aglutinan el objeto del reglamento (art. 1 PCE-RGPD), el ámbito de aplicación (art. 2 y 3 PCE-RGPD) y las definiciones (art. 4 PCE-RGPD). En el Capítulo II se recogen los principios que incluirían los principios de calidad en la Directiva 95/46/CE (art. 5 PCE-RGPD), las bases jurídicas que legitiman el tratamiento de datos en general (art. 6 PCE-RGPD) y de categorías especiales (art. 7 PCE-RGPD), así como una nueva disposición sobre el tratamiento de datos específico de menores (art. 8 PCE-RGPD) y una referencia a evitar tratamientos de datos personales ocasionados únicamente por el cumplimiento del reglamento (art. 10 PCE-RGPD).

En el Capítulo III se incluyen los derechos del interesado que se amplían y refuerzan. Así el deber de informar se amplía con el principio de transparencia (art. 11 PCE-RGPD) y con un contenido más extenso de la obligación que se adapta al entorno digital (art. 14 PCE-RGPD). El derecho de acceso incluye, además del acceso a la información, la obtención de la misma para permitir la portabilidad de los datos, de forma que también se muestra esta adaptación al entorno digital (art. 15 PCE-RGPD). También se ha desarrollado ostensiblemente la regulación del derecho a la supresión (art. 17 PCE-RGPD), se ha ampliado

[1552] Los textos del Parlamento y del Consejo UE modifican la propuesta de la Comisión. Cuando me refiera al texto de la Comisión (PCE-RGPD) será porque no ha habido cambios en el proceso legislativo o porque me refiero a este texto para compararlo con los del Parlamento y del Consejo UE. Se puede consultar una comparativa de los tres textos en: *Note from Presidency to Working Group on Information Exchange and Data Protection (DAPIX). Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Interinstitutional file: 2012/0011(COD) 10391/15, Council of the EU, Brussels, 8.7.2015.*

[1553] Frente a los 72 considerandos y 34 artículos de la Directiva, el PCE-RGPD contiene 139 considerandos y 91 artículos. El número seguramente será mayor, ya que en los textos del Parlamento y del Consejo UE se han añadido artículos, que no se reflejan en estos números.

el derecho de oposición (art. 19 PCE-RGPD) y se ha otorgado gran importancia al denominado derecho relativo a la elaboración de perfiles (art. 20 PCE-RGPD), que sustituye la denominación de la Directiva 95/46/CE de decisiones individuales automatizadas.

El Capítulo IV es el que recoge principalmente el estatuto del responsable del tratamiento y del encargado del tratamiento y que abordaré con más detenimiento en el próximo apartado (arts. 22 ss. PCE-RGPD). También incluye, no obstante, la regulación de la figura del delegado de protección de datos y la de los códigos de conducta y la certificación.

El Capítulo V establece la regulación de las transferencias internacionales de datos en la que fundamentalmente se han incorporado los nuevos mecanismos ideados por las autoridades de protección de datos para flexibilizar las mismas en el nuevo contexto (art. 40 ss. PCE-RGPD). El Capítulo VI y VII se refieren a la parte institucional sobre las autoridades de control y los mecanismos de cooperación.

El Capítulo VIII es otro de gran importancia para la figura del responsable ya que contempla los recursos (art. 73 a 76 PCE-RGPD), la responsabilidad (art. 77 PCE-RGPD) y las sanciones (art. 78 y 79 PCE-RGPD). El Capítulo IX recoge las disposiciones relativas a situaciones de tratamiento de datos específicas, de forma que establece habilitaciones para que los Estados miembros legislen sobre determinadas materias como son la libertad de expresión (art. 80 PCE-RGPD), la salud (art. 81 PCE-RGPD), el derecho laboral (art. 82 PCE-RGPD), la seguridad social (art. 82bis PCE-RGPD), la investigación (art. 83 PCE-RGPD), los servicios de archivo (art. 83bis PCE-RGPD), deber de secreto (art. 84 PCE-RGPD) y las normas sobre iglesias y asociaciones religiosas (art. 85 PCE-RGPD). Finalmente, el Capítulo X se refiere a los actos delegados y de ejecución que servirán para desarrollar el reglamento y el Capítulo XI contiene las disposiciones finales.

2. LA REFORMA Y EL RESPONSABLE

En la PCE-RGPD se confirma el papel esencial que se atribuyó al responsable en la Directiva 95/46/CE, es decir, elemento determinante del ámbito de aplicación de la norma, sujeto obligado y aglutinador de la responsabilidad. Este papel se mantiene aunque, evidentemente, se transforma, en una nueva norma que, al ser de aplicación directa, tiene un mayor desarrollo que la Directiva 95/46/CE.

2.1. El concepto inalterado en un ampliado ámbito de aplicación

2.1.1. El concepto inalterado

Lo primero que hay que destacar es la permanencia inalterada del concepto del responsable del tratamiento con una excepción. En la PCE-RGPD se había introducido un pequeño cambio en los aspectos concretos sobre los que ejercía el poder de control el responsable, ya que se había añadido a los fines y medios, otro aspecto: "las condiciones"[1554]. Sin embargo, tanto, en el texto del Parlamento, como en el del Consejo UE se ha eliminado, por lo que ambas instituciones han preservado la definición establecida en la Directiva 95/46/CE[1555]. Tampoco se ha planteado la sustitución de la conjunción "y" por la "o" en los "fines y medios", como ya he sugerido, en su momento, para clarificar que se puede calificar a un responsable por determinar cualquiera de los dos aspectos[1556].

Por otro lado, también hubo algunas propuestas dirigidas a simplificar estos aspectos, de forma que sólo se dejaran "los fines", como elemento esencial para calificar al responsable[1557]. Sin embargo, finalmente no se acogieron. La argumentación para

[1554] Según el Supervisor Europeo de Protección de Datos, el término "condiciones" pondría más enfásis en la responsabilidad de quienes determinaran cómo se organiza concretamente la actividad del tratamiento. Esta interpretación, según el Supervisor, facilitaría la atribución de responsabilidad al proveedor de servicios de *cloud computing*. *Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", 16.11.2012*, pág. 13.

[1555] Así se justificó en la enmienda 744. Enmiendas (2) 602 – 885, Proyecto de informe Jan Philipp Albrecht (PE501.927v04-00) sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) Propuesta de Reglamento, (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 4.3.2013.

[1556] Ver Capítulo II.

[1557] En la enmienda 748, en la justificación se alude a lo indicado por el Comité de Industria, Investigación y Energía. En las enmiendas recogidas en ese comité se justificaba la eliminación de los términos "condiciones y medios" y, por tanto, la exclusiva mención de los fines, para clarificar la distinción entre responsable del tratamiento y encargado del tratamiento. De esta forma, en la enmienda 335 se argumentaba que el responsable del tratamiento es el que determina el "porqué" del tratamiento, mientras que el encargado, es el que determina las condiciones y los medios. Esta argumentación variaría el concepto, ya que le otorgaría al encargado el poder de determinar los medios, sean esenciales o no. La enmienda 336, pese a contemplar la misma modificación, utiliza una argumentación más acorde con la interpretación del concepto de la Directiva 95/46/CE porque, aunque lo que pretende es la diferenciación entre las figuras de responsable y encargado, lo que aduce es que la definición del responsable debería fundamentarse en la decisión sobre los fines, más que en la decisión sobre los medios. No establece, por tanto, la separación de los elementos sino que estima que debe pesar más en la definición del responsable la decisión sobre los fines, que sobre los medios. Asimismo, indica que son los fines los que también deberían guiar el reparto de responsabilidades, cuando hubiera varios responsables. Enmiendas 746 a 748, *Ibídem* y Enmiendas 334 a 336, *Amendments 165 – 356, Draft opinion Seán Kelly(PE496.562v01-00) on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the*

establecer sólo los fines, como aspecto concreto sobre el que el responsable debe tener la capacidad de determinar, era principalmente que facilitaría su distinción con el encargado. El encargado del tratamiento, como se verá, asume, en el reglamento, un papel mucho más relevante que el que tenía en la Directiva 95/46/CE. A esto hay que añadir la dificultad experimentada en la práctica a la hora de diferenciar al responsable del encargado.

Como los fines claramente apuntan a la caracterización del responsable y era la determinación de los medios lo que originaba la mayor problemática, se ha querido eliminar este factor controvertido. Sin embargo, esto significaría que el encargado podría determinar los medios, fueran esenciales o no, lo que llevaría a una concepción de control compartido y desnaturalizaría el concepto de encargado.

Se reproduce la definición de la PCE-RGPD:

> **"**«responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines, condiciones y medios del tratamiento de datos personales; en caso de que los fines, condiciones y medios del tratamiento estén determinados por la legislación de la Unión o de los Estados miembros, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por la legislación de la Unión o de los Estados miembros;" (art. 4.5 PCE-RGPD).

Sin duda, dice mucho de la vigencia de la figura el que se haya conservado intacta en el reglamento su definición[1558]. También hay que concluir que el análisis extraído de

---

processing of personal data and on the free movement of such data, Proposal for a regulation, (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 20.12.2012. Respecto al trámite en el Consejo UE, la República Checa sugirió eliminar el término "medios" del concepto. *Note from General Secretariat of the Council to Delegations on the Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)-Preparation of a general approach, Interinstitutional File: 2021/0011 (COD) 9788/15, Council of the EU, Brussels, 11.6.2015.*

[1558] No se encuentran muchas críticas al concepto. Se puede citar la realizada por *House of Lords* en un informe relativo a la Sentencia del TJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2014:317. La Cámara inglesa considera que la definición debería actualizarse en el PRGPD, ya que, al igual que sucede con la Directiva 95/46/CE en su conjunto fue concebida en un momento, el año 1995, en el que aún no existían los buscadores en Internet y, por lo tanto, la definición no debería dar cabida a los mismos. Sin embargo, no se ofrece ninguna argumentación que apoye esta crítica, ni tampoco se propone una definición alternativa. Entiendo que remite a los argumentos esgrimidos por el Abogado General Niilo Jääskinen en sus conclusiones, ya que es lo que hizo Neil Cameron, un consultor que fue preguntado en la cámara, y que remitió a la fundamentación del Abogado General para considerar que *Google* no debía ser calificado de responsable del tratamiento. También el Profesor L. Floridi fue entrevistado y criticó los conceptos de responsable y de encargado del tratamiento, pero en realidad lo que argumentó es que la definición de "tratamiento" era tan amplia que cualquiera que haga algo con los datos acaba siendo calificado de

los elementos del concepto (subjetivo, objetivo y funcional) sigue siendo válido, si bien habrá que tener en cuenta, especialmente, las novedades relativas al ámbito de aplicación que se expondrán en el siguiente punto.

Por tanto, se puede mantener la conclusión derivada del análisis del concepto de la Directiva 95/46/CE y es que la simplicidad del concepto logra ampliar su ámbito a un gran número de sujetos. Este hecho que puede considerarse una fortaleza, es, a su vez, una debilidad ya que permite realizar un análisis poco consistente, si no se sigue una sistemática coherente en todos los supuestos, como se deduce de la práctica actual.

La expresión "solo o conjuntamente" que, al igual que sucede en la Directiva 95/46/CE alude a la posibilidad de que existan varios responsables, se repite en la definición que se ha incorporado en la PCE-RGPD de encargado del tratamiento. Además, se ha añadido una regulación de la corresponsabilidad que no hace sino reflejar la interpretación del GA29 sobre la importancia de que los corresponsables asignen formalmente las responsabilidades o, en caso contrario, se presuma que la responsabilidad sea solidaria[1559].

El concepto en el reglamento mantiene, en consecuencia, su validez. El responsable, mantiene su papel clave en esta norma, aunque lo comparte con el encargado del tratamiento, que ha adquirido una mayor relevancia y responsabilidad. Por eso, se confirma la existencia de ambos conceptos por su papel delimitador, para diferenciar una figura de la otra. Asimismo, en el reglamento se incide especialmente en regular la corresponsabilidad en un contexto digital, en el que ya hemos visto que es esencial poder asignar responsabilidades a los diversos participantes en el mismo.

---

responsable. Finalmente, en sus conclusiones, la *House of Lords* repite un argumento utilizado por el Abogado General, que había alegado que, si se considerara que *Google* era responsable del tratamiento, debería considerarse que todos los que navegan por Internet y se descargan archivos, son responsables del tratamiento. Por eso la cámara inglesa recomienda que se modifique la definición para evitar esta inclusión. Sin embargo, habría que tener en cuenta las exclusiones como la relativa a la actividad doméstica que evitarían la aplicación de la normativa, pese a que pudiera en un inicio considerarse responsable a cualquier sujeto. *EU data protection law: a "right to be forgotten"?, House of Lords, European Union Committee, 2nd Report of Session 2014-15, ordered to be printed 23 July 2014 and published 30 July 2014*, págs. 8, 13 a 14, 21 a 22 y *European Union Committee, Home affairs, health and education sub-committee, EU data protection law: a "right to be forgotten"? Evidence*, págs. 3 y 18.

[1559] Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.* pág. 27.

Se han incluido otras definiciones relacionadas con los conceptos de responsable y encargado relativas al establecimiento principal, el representante, empresa y grupo de empresas (art. 4, apdos. 13 a 16 PCE-RGPD). Las mismas sirven de base, especialmente, en la determinación de la autoridad de control competente para conocer de los asuntos que puedan plantearse sobre incumplimientos o trámites en el reglamento. Al establecer una regulación única uniforme se han querido simplificar los trámites para los responsables que se ubican en varios Estados miembros, de forma que se relacionen con una única autoridad. Para ello, se ha incorporado un mecanismo de cooperación entre las autoridades que ha originado una gran complejidad en la regulación, con el fin de determinar la competencia de las mismas.

Respecto a los otros sujetos que se definían en la Directiva 95/46/CE, hay que decir que el texto inicial incluyó el de destinatario (art. 4.7 PCE-RGPD), pero no el de tercero[1560]. El Parlamento introdujo este último, tal cual estaba en la Directiva 95/46/CE (art. 4.7bis PPE-RGPD).

2.1.2. Un ámbito de aplicación ampliado

a. El ámbito de aplicación material

El ámbito de aplicación general se mantiene, al igual que en la Directiva 95/46/CE, a los tratamientos total o parcialmente automatizados y a los tratamientos no automatizados de datos contenidos o destinados a ser incluidos en un fichero (art. 2.1 PCE-RGPD). También permanecen, casi sin variaciones, los conceptos de fichero y tratamiento (art. 4.3 y .4 PCE-RGPD).

No obstante, el Parlamento y el Consejo UE han incluido la definición de lo que consideran "elaboración de perfiles" debido a la relevancia adquirida en su utilización en el contexto de Internet (art. 4.3bis PPE-RGPD y 4.12bis PCJ-RGPD). El Consejo UE ha definido los tratamientos relativos a la "restricción de tratamiento" y la "seudonimización" (art. 4.3bis y .3ter PCJ-RGPD). Esta última operación correspondería al bloqueo de la Directiva 95/46/CE, aunque se ha optado por esta nueva rúbrica para

[1560] El Consejo UE modificó la definición de destinatario de la PCE-RGPD, para igualarla a la de la Directiva 95/46/CE, ya que la Comisión había eliminado la última parte de la misma que excluía de la definición a las autoridades que pudieran recibir datos, en el marco de una investigación.

evitar las connotaciones negativas del término bloqueo[1561]. Asimismo, también el texto del Consejo UE incorpora la definición de lo que se considera "tratamiento transnacional", con el fin de facilitar la determinación de la autoridad de control competente (art. 4.19ter PCJ-RGPD).

Como ya se ha indicado anteriormente, el reglamento no se aplicará a los tratamientos de datos realizados en actividades no sujetas al derecho de la Unión ni se aplicará a los tratamientos realizados por los Estados miembros, cuando lleven a cabo actividades relativas a la política exterior y de seguridad común (art. 2.2.a) y c) PCE-RGPD). Respecto a las actividades que se entendían no comprendidas en el ámbito de aplicación del derecho de la Unión, en el texto inicial se especificaba que una de ellas era la seguridad nacional. Tanto el Parlamento, como el Consejo UE eliminaron esta concreción del precepto, si bien el Consejo lo ha mantenido en la parte del preámbulo (Considerando 14 PCJ-RGPD).

El reglamento tampoco se aplicará a los tratamientos que realicen las autoridades públicas con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, ya que estos se regularán por la PCE-Directiva policía (art. 2.2.e) PCE-RGPD). En el texto del Consejo UE se añadieron los fines relativos a la protección y prevención frente a las amenazas a la seguridad pública, con el fin de alinearse con el texto en trámite de elaboración de la Directiva policía.

También se incorpora la interpretación que realizó la sentencia *Lindqvist* en lo relativo a las actividades personales o domésticas que se extraen del ámbito de aplicación[1562]. El Parlamento la introduce, al indicar que esta excepción también se aplicará a la publicación de datos personales, cuando quepa esperar razonablemente que solo accedan a ella un número limitado de personas (art. 2.2.d) PPE-RGPD). El Consejo UE ha preferido incluir una referencia más general, en la parte del preámbulo, donde entiende que la exclusión se refiere también a las redes sociales y la actividad en línea

[1561] *Note from General Secretariat of the Council to Delegations on the Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)-Preparation of a general approach, Interinstitutional File: 2021/0011 (COD) 9788/15, Council of the EU, Brussels, 11.6.2015.*

[1562] Sentencia del TJUE de 6 de noviembre de 2003 *Bodil Lindqvist*, C-101/01, EU:C:2003:596.

realizada en el contexto de las actividades personales y domésticas (Considerando 15 PCJ-RGPD).

Todos los textos son unánimes en cuanto a aplicar a los responsables o encargados, que proporcionen los medios para el tratamiento, relacionado con estas actividades personales o domésticas, el reglamento (Considerando 15 PCE-RGPD)[1563].

Es interesante la referencia, en el ámbito de aplicación material, a las normas en materia de responsabilidad de los prestadores de servicios intermediarios, de forma que da a entender que será aplicable lo indicado en esta regulación de la Directiva 2000/31/CE (art. 2.3 PCE-RGPD). Así, las exclusiones de responsabilidad que esta norma contiene respecto a estos actores específicos del mundo de Internet se confirma que serán también válidas en materia de protección de datos.

Sin embargo, el Consejo UE ha eliminado el texto del precepto y ha optado por referirse a esta Directiva 2000/31/CE en la parte de Considerandos (Considerando 17 PCJ-RGPD). En la misma, aclara que ambas regulaciones, la del reglamento y la Directiva 2000/31/CE deben aplicarse de forma independiente. Esto responde a las dudas de algunos Estados, al respecto de la obligación establecida para los responsables de suprimir los datos que hubieran hecho públicos, en caso de que un interesado ejerciera su derecho a la supresión o al olvido, y de notificarlo a otros responsables que trataran esos datos (art. 17.2a PCJ-RGPD)[1564].

El concepto de dato personal, en el texto inicial, se define como la información relativa a un interesado (art. 4.2 PCE-RGPD). Por ello, se debía acudir a la definición de este interesado (art. 4.1 PCE-RGPD) para saber si podíamos estar ante un dato personal. La definición era muy similar a la que proporcionaba la Directiva 95/46/CE. Esto se modifica en los textos del Parlamento y del Consejo UE, para aunar estos conceptos en

[1563] Si bien esta disposición apunta claramente a los prestadores de servicios de redes sociales, también dará cabida a otros supuestos, como la videovigilancia llevada a cabo por particulares.
[1564] *Note from General Secretariat of the Council to Delegations on the Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)-Preparation of a general approach, Interinstitutional File: 2021/0011 (COD) 9788/15, Council of the EU, Brussels, 11.6.2015.*

uno solo, relativo a los datos personales, como se establecía en la Directiva 95/46/CE (art. 4.2 PPE-RGPD y PCJ-RGPD).

Además de este cambio, ambas instituciones incluyen una alusión clara a los identificadores, como datos que permitirán determinar la identidad de una persona (nombre, número de identificación, datos de localización). Sin embargo, en el entorno de Internet, se precisa, en todos los textos que los identificadores, como las controvertidas direcciones IP, no se calificarán automáticamente como datos personales, en todas las circunstancias (Considerando 24 PCE-RGPD).

Otra novedad del reglamento es la introducción de los criterios que proporcionó el GA29 para realizar la valoración sobre cuándo puede considerarse que una persona es identificable (Considerando 23 PCE-RGPD). El responsable deberá valorar los medios que puedan ser razonablemente utilizados por él mismo o por cualquier otro individuo para identificar o distinguir directa o indirectamente a dicha persona. Además se introducen unos criterios para determinar esta razonabilidad, de forma que deben tenerse en cuenta todos los factores objetivos, como los costes o tiempo necesarios para la identificación. Asimismo, se debe valorar la tecnología disponible en el momento del tratamiento y también el desarrollo tecnológico.

Se incentiva especialmente el uso de datos seudónimos, como una garantía de la protección de los datos, que desarrolla ampliamente el Consejo UE, en su propuesta (art. 4.3ter y Considerandos 23 ss. PCJ-RGPD). Asimismo, se aclara en este texto, la diferenciación con el proceso de anonimizar los datos, que permitirá excluir la aplicación del reglamento, mientras que el uso de seudónimos deja intacta la aplicación del resto de principios del reglamento (Considerandos 23 y 23bis PCJ-RGPD).

Respecto a los datos, se han incorporado algunas definiciones complementarias. En los tres textos se establecen, aunque con variaciones las relativas a: “datos genéticos”, “datos biométricos” y “datos relativos a la salud” (art. 4 apdos. 10 a 12 PCE-RGPD). El Parlamento incluye las de “datos cifrados” y “datos seudónimos” (art. 4.2bis y .2ter PPE-RGPD).

Por último, indicar que se deja claro que no se protegerá el tratamiento de datos relativos a personas jurídicas y se incorpora como novedad que tampoco se incluirán en esta protección sus datos de contacto (Considerando 12 PCE-RGPD).

b. El ámbito de aplicación territorial

Si hay una novedad importante en el ámbito de aplicación es, sin duda, la relativa a la aplicación territorial de la norma. Se ha dado respuesta a las demandas que se habían realizado para ampliar la aplicación a responsables localizados fuera de la UE, sin tener que acudir a criterios forzados, como se relataba en el anterior capítulo respecto al asunto *Google*.

Así, se han mantenido dos de los criterios establecidos por la Directiva 95/46/CE para aplicar la norma. El primero es el relativo a la aplicación en casos en los que el responsable está ubicado en un lugar donde se le aplica el derecho de un Estado miembro en virtud de normas de derecho internacional público que no había suscitado problemas (art. 3.3 PCE-RGPD). El segundo es el supuesto en el que el tratamiento de datos se realice en el contexto de las actividades de un establecimiento del responsable en la UE, aunque se ha añadido también el establecimiento de un encargado del tratamiento (art. 3.1 PCE-RGPD). El Parlamento añadió a este criterio que, se aplicaría el reglamento, independientemente de que el tratamiento tuviera lugar o no en la UE (art. 3.1 PPE-RGPD).

El tercer criterio que se incluía en la Directiva 95/46/CE era el que hacía referencia al recurso a medios ubicados en el territorio de la UE, por parte de un responsable ubicado fuera de este territorio. Pues bien, este criterio se cambia por el que había sido reivindicado por las autoridades de control y que respondía al actual contexto digital[1565]. El reglamento se aplicará al tratamiento de datos de interesados en la UE, que

[1565] El GA29 ya había sugerido que se incorporara un nuevo criterio de conexión que tuviera en cuenta la orientación hacia las personas como el establecido por la legislación sobre la protección de los menores en Internet de Estados Unidos (*Children's Online Privacy Protection Act* o COPPA) o algunas legislaciones nacionales europeas que, al transponer la Directiva 2000/31/CE sobre el comercio electrónico, habían establecido dentro del ámbito de aplicación los servicios que se orientaran a los territorios de los Estados miembros. Esto sucedía con la ley española, la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, en su artículo 4. Dictamen 8/2010 sobre derecho aplicable, *op. cit.*, pág. 28

realice un responsable no establecido en la Unión, si las actividades de tratamiento se relacionan, o con la oferta de bienes y servicios a dichos interesados en la Unión, o con el control de su conducta (art. 3.2 PCE-RGPD).

El Parlamento incluyó que también se aplicaría este criterio al tratamiento que realizara un encargado no establecido en la UE, que la oferta de bienes o servicios no era necesario que implicara pago por parte del interesado y cambió "el control de su conducta" por "el control de los interesados" (art. 3.2 PPE-RGPD). El Consejo UE, por su parte, delimitó la conducta del interesado sometida a control, de forma que precisó que esta debía tener lugar en la UE (art. 3.2 PCJ-RGPD).

Como se puede observar, se ha ampliado el ámbito de actuación de forma que, por ejemplo, en el asunto *Google*, la empresa estadounidense se sometería claramente a la aplicación del reglamento. No obstante, se introducen elementos que están abiertos a la interpretación y sobre los que se han incorporado algunos criterios. ¿Cuándo se considera que se ofrecen bienes o servicios a los interesados en la UE? El Parlamento indicó que debía averiguarse si era evidente que el responsable se planteara esta opción (Considerando 20 PPE-RGPD). El Consejo UE indica algunos criterios que pueden reflejar esta intención, como el uso de una lengua o una moneda utilizada generalmente en los Estados miembros o la mención de clientes o usuarios residentes en la UE (Considerando 20 PCJ-RGPD)[1566].

Respecto a la alusión al control de la conducta de los interesados ¿qué debe entenderse por control? En el texto inicial de la Comisión, se definía controlar la conducta como el seguimiento de individuos en Internet al aplicar perfiles a individuos para adoptar decisiones o analizar o predecir sus preferencias, comportamientos o actitudes (Considerando 21 PCE-RGPD). En el texto del Parlamento se mantienen esas mismas finalidades pero se incide en que será independiente del origen del que se extraigan los datos y aunque el uso con esa finalidad fuera posterior. Respecto a este último cambio, quizás responda a la sugerencia realizada por el GA29 para ampliar los tratamientos incluidos en esta actividad de control, de forma que no deban ser estrictamente los

[1566] No considera que sean suficientes para determinar esta intención del responsable, la simple accesibilidad del sitio web del responsable o de un intermediario en la UE o de una dirección de correo electrónico y otros datos de contacto, o el uso de una lengua generalmente utilizada donde resida el responsable (Considerando 20 PCJ-RGPD).

destinados a crear perfiles, sino que puedan incluirse otros que también se consideren una monitorización del comportamiento[1567].

Respecto a este criterio, también quiero hacer mención de la obligación que tendrán los responsables de fuera de la UE de designar representante en la UE y que abordaré más adelante.

2.2. Un nuevo estatuto para el responsable

Si se analiza la asignación de obligaciones, al igual que se analizó en la Directiva 95/46/CE, lo primero que se observa es que la mayoría de éstas se atribuyen de forma expresa. Es decir, consta explícitamente que el responsable debe cumplir la obligación en concreto. Ello se debe fundamentalmente a que el Capítulo IV del reglamento establece un estatuto específico para el responsable y también para el encargado del tratamiento. Así, las pocas obligaciones detectadas de asignación implícita se encuentran en otros capítulos del reglamento.

Cuando analicé las diversas obligaciones del responsable, enunciadas en la Directiva 95/46/CE, opté por exponerlas según la fase del ciclo del tratamiento en la que se localizaban: entrada, salida o aplicación transversal a todo el ciclo. En el reglamento se aprecia la intención de transversalidad en la mayoría de los preceptos y, especialmente, en la parte relativa al responsable del tratamiento[1568].

Iniciaré la revisión de las obligaciones del responsable con aquellas que se encuentran en la parte del reglamento dedicada al responsable, en lo que entiendo es su nuevo estatuto (Capítulo IV PCE-RGPD). Al ser una de las principales novedades del reglamento, me detendré, especialmente, en el principio de rendición de cuentas (principio de *accountability*) (art. 5.1.f) PCE-RGPD). Como se verá no es un principio nuevo, sino que ya se encontraba en otros instrumentos jurídicos y su incorporación había

[1567] Dictamen 01/2012 sobre las propuestas de reforma de la protección de datos, 00530/12/ES WP 191, 23.3.2012, Grupo de trabajo Artículo 29 sobre la protección de datos, pág. 9.

[1568] El GA29 ha considerado positivo que se incentive al responsable para que proteja el derecho a la protección de datos, desde un inicio y durante todo el ciclo de vida del tratamiento, al establecer las evaluaciones de impacto o los principios de protección de datos desde el diseño o protección de datos por defecto, así como la obligación de *accountability.* Dictamen 01/2012 sobre las propuestas de reforma de la protección de datos, *op. cit.*, pág.4.

sido sugerida, ya por el GA29 para mejorar el cumplimiento de las obligaciones de protección de datos. Este principio se complementa, de forma natural con la elaboración de códigos de conducta y con la certificación.

Tras examinar el principio de *accountability*, abordaremos el resto de obligaciones del nuevo estatuto del responsable. No distinguiré entre las fases del ciclo, ya que prácticamente todas tienen carácter transversal. Si acaso las que podrían considerarse previas al tratamiento son la evaluación de impacto y la autorización y consulta previas.

La designación del delegado de protección de datos y del representante del responsable, la relación con el encargado del tratamiento y la corresponsabilidad, que también se incluyen en este nuevo estatuto del responsable, muestran la importancia de la participación de diversos implicados en la regulación del derecho de protección de datos.

Por último, haré una referencia a aquellas obligaciones que derivan de los principios relativos al tratamiento de datos, de los derechos de los interesados y de la regulación de las transferencias internacionales de datos.

2.2.1. Un impulso a la autorresponsabilidad: de la introducción de la accountability a la certificación

El GA29, en su documento sobre "El futuro de la privacidad"[1569], estimaba que la Directiva 95/46/CE no había conseguido que se aplicaran mecanismos eficaces para garantizar la protección de los datos. Por tanto, el GA29 sugería que se incluyera en la revisión de la Directiva 95/46/CE un principio de responsabilidad, que exigiera que los responsables del tratamiento dispusieran de los mecanismos internos necesarios para demostrar el cumplimiento de los principios y obligaciones establecidos por la directiva a interesados, como las autoridades de control[1570]. Este principio que se ha traducido al

[1569] El futuro de la privacidad, contribución conjunta a la consulta de la Comisión Europea sobre el marco jurídico del derecho fundamental a la protección de datos de carácter personal, 02356/09/ES, WP 168, de 1.12.2009, Grupo de trabajo Artículo 29 sobre la protección de datos y Grupo de trabajo Policía y justicia.

[1570] El Supervisor Europeo de Protección de Datos también ha formulado una definición de este principio: *"Accountability: Principle intended to ensure that controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice. Accountability requires that controllers put in place internal mechanisms and control systems that ensure compliance and provide evidence – such as audit reports – to demonstrate compliance to external stakeholders, including*

español como de responsabilidad, puede confundirse con la responsabilidad civil. Por ello, me referiré al mismo con el término en inglés *accountability*.

El GA29 analizó con más detenimiento este principio de *accountability* en un dictamen en el año 2010[1571]. En este documento, que servía de preparación a la reforma que estaba en ciernes del marco jurídico regulador del derecho a la protección de datos, el GA29 proponía la inclusión del principio, que constaría de dos elementos esenciales: la necesidad de que el responsable adoptara medidas adecuadas y eficaces para aplicar los principios de protección de datos, y la necesidad de demostrar, si fuera requerido, que se han adoptado estas medidas adecuadas y eficaces.

¿Qué es lo que persigue este principio? Lo que se busca con la *accountability* es, como indicaba el GA29, la progresión en materia de protección de datos de la teoría a la práctica. Se quiere alcanzar la eficiencia en el cumplimiento de la protección de los datos personales, que contemple la necesaria evolución en la tecnología, sea flexible y que permita a organizaciones en múltiples territorios y jurisdicciones cumplir de forma uniforme en todas sus ubicaciones, sin disminuir por ello la protección.

Independientemente de su formulación expresa como tal principio, la *accountability* es una pieza más en la tendencia existente hacia la incorporación en la regulación de fórmulas de autorresponsabilidad[1572]. Los responsables se convierten así en elemento estratégico en el sistema de garantías del derecho a la protección de datos[1573]. De esta forma, el legislador adopta un enfoque que tenga en cuenta la naturaleza internacional, global y tecnológica del derecho a la protección de datos. Al no poder hacer frente a la complejidad que acarrean estas características mediante la perspectiva tradicional de la normativa, de forma natural se han incorporado mecanismos de autorregulación, como ha sucedido con la adopción de las *Binding Corporate Rules* o con

supervisory authorities." https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/71#accountability (fecha consulta: 26.3.2015).

[1571] Dictamen 3/2010 sobre el principio de responsabilidad, 00062/10/ES, GT 173, de 13.7.2010, Grupo del Trabajo del Artículo 29.

[1572] Ver Capítulo VII.

[1573] A. TRONCOSO REIGADA, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *Revista Española de Derecho Europeo*, *op. cit.*, pág. 25.

el impulso de estándares o certificaciones, tanto a nivel europeo, como a nivel nacional[1574].

La autorresponsabilidad promueve un cumplimiento más eficaz de la normativa y traslada el momento de supervisión de las autoridades que, en vez de ser previo al tratamiento será posterior, en caso de que exista un problema de incumplimiento. Es más, el principio de *accountability* llevado al máximo lo que pretende es que sea el mismo responsable el que supervise y repare el incumplimiento, sin necesidad siquiera de la intervención de la autoridad de control. En todo caso, al incentivar una mejora en la gestión del cumplimiento normativo, lo que se hace es acentuar la prevención de la vulneración de los derechos. Ahora bien, la autorregulación no puede ser la solución única a la protección de los ciudadanos sino complementaria a la acción de quienes deben regular y supervisar[1575]. No hay que olvidar que las empresas se mueven por una lógica económica a corto plazo[1576].

a. Un principio ya existente en diversos instrumentos jurídicos

El principio de *accountability* no es nuevo. Así, en Europa se puede extraer algún germen del mismo en la Directiva 95/46/CE, donde se especifica, respecto a los principios de calidad de los datos que "corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1" (art 6.2 Directiva 95/46/CE)[1577] y también cuando se establece la obligación de aplicar medidas técnicas y organizativas (art. 17.1 Directiva 95/46/CE)[1578]. Y, si bien no se establece en el texto de la Directiva 95/46/CE, un ejemplo de aplicación de este principio es, como se ha indicado, el de las *Binding Corporate Rules*, que desarrolló el GA29 para facilitar la realización de transferencias internacionales de datos, en el ámbito de grupos de empresas[1579].

[1574] Ver Capítulo V y VI.
[1575] A. TRONCOSO REIGADA, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *Revista Española de Derecho Europeo*, *op. cit.*, pág. 26.
[1576] *Ibídem*, pág. 143.
[1577] Ya se ha indicado que el Consejo UE ha eliminado la referencia expresa al principio de *accountability* pero ha incluido de nuevo esta fórmula de la Directiva 95/46/CE.
[1578] Dictamen 3/2010, sobre el principio de responsabilidad, *op. cit*., págs. 8 a 9.
[1579] Ver Capítulo V. Dictamen 3/2010, sobre el principio de responsabilidad, *op. cit*., págs. 7 y 17.

Las multinacionales debido a su tamaño y a esa deslocalización tienen que lidiar con numerosas normativas que deben cumplir en cada uno de los países en los que se ubican sus empresas. Algunas de estas normativas exigen que se adopten políticas internas y procedimientos, como sucede en el blanqueo de capitales o en el sector financiero. Además, deben contar con las diferencias culturales de las personas que conforman las plantillas o que son clientes o proveedores.

Todos estos factores han obligado a estas empresas a adoptar un enfoque de cumplimiento normativo, en el que han establecido su propia normativa interna. De esta forma, al aplicar una normativa propia, consiguen armonizar toda la gestión en las diferentes ubicaciones y facilitan el cumplimiento. Evidentemente, para que este sistema funcione, el nivel de exigencia de esta normativa interna debe ser elevado y debería atender a la normativa más estricta que, en un determinado sector o materia, la empresa deba cumplir.

Las autoridades de control decidieron aprovechar este sistema y diseñaron un procedimiento, mediante el cual el grupo de empresas podía acudir a una sola de las autoridades y con la adopción de estas reglas internas asegurar que todas las empresas del grupo respeten esta normativa. De esta forma, el grupo de empresas crea un ámbito en el que se asegura el nivel adecuado de protección. Este sería un sistema que se fundamenta en el principio de *accountability*, pues lo que pretende es que el grupo de empresas, además de cumplir con la normativa en materia de protección de datos, sea capaz de demostrarlo en el trámite que debe realizar ante las autoridades de control.

Este principio ya se reconocía, de forma expresa, en la Guía OCDE 1980 y se expresaba de la siguiente manera: "Todo responsable de datos debería ser responsable de cumplir con las medidas que hagan efectivos los principios [materiales] expuestos"[1580]. Esta guía se actualizó en el 2013 y en esta nueva versión, además de permanecer el principio sin cambios, se añadió un desarrollo del mismo que refleja la importancia que

[1580] Esta disposición se incluía en el parágrafo 14 de la Guía, en la parte dedicada a los principios básicos de aplicación nacional, y en la versión inglés se expresa como sigue: "*accountability principle: a data controller should be accountable for complying with measures which give effect to the principles stated above*".

ha adquirido en esta materia[1581]. También se recoge el principio en otro instrumento jurídico internacional inspirado en la Guía de la OCDE, como es el APEC Privacy Framework[1582]. Hay que recordar que, al igual que la Guía OCDE, se trata de un instrumento no vinculante para los Estados parte.

Respecto a las legislaciones, el principio de *accountability* se ha incluido de forma expresa en la Ley canadiense de protección de información personal y documentos electrónicos (Ley canadiense)[1583] y en la legislación federal mexicana (Ley mexicana y Reglamento de desarrollo de la Ley mexicana)[1584].

[1581] De esta forma, en la guía se añade una tercera parte titulada: *implementing accountability* que incluye el desarrollo de este principio en su parágrafo 15. *Recommendation of the Council concerning Guidelines governing the protection of privacy and transborder flows of personal data (2013), C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79*. http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (fecha consulta: 21.7.2014). El informe adicional, que se adjunta a la revisión de 2013 de la guía (*supplementary explanatory memorandum*), así como el informe del grupo de trabajo que se encargó de la misma, destacan la importancia del principio de *accountability*. El grupo de trabajo, en su segunda reunión, abordó la cuestión de la aplicación proactiva y el cumplimiento, que incluyó propuestas sobre la *accountability* de las organizaciones, las notificaciones de incidencias de seguridad y el refuerzo del cumplimiento. OECD (2013), "*Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines*", OECD Digital Economy Papers, No. 229, OECD Publishing, pág. 6. http://dx.doi.org/10.1787/5k3xz5zmj2mx-en (fecha consulta: 8.8.2014).

[1582] Ver Capítulo I. El APEC Privacy Framework incluye como el de *accountability*: "*A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.*" APEC Privacy Framework, Principio IX, (punto 26).

[1583] Canadá es un Estado federal, por lo que tiene normas de protección de datos a nivel federal y también a nivel de los diferentes Estados. En 1977 Canadá promulgó la primera regulación federal sobre protección de datos que se centraba en el sector público y que se hallaba en la Parte IV de la Ley canadiense sobre los derechos de la persona (*Canadian Human Rights Act*). En 1983 se aprobó la *Privacy Act* que incluía esta regulación del sector público. En 1984 Canadá manifestó su compromiso de cumplir la Guía de la OCDE de 1980. Sin embargo, la ley federal no se refería al sector privado y la autoridad de control canadiense (el *Privacy Commissioner*) solicitó al gobierno que se incentivara por ley el desarrollo de códigos de conducta para este sector. La entidad *Canadian Standards Association* (CSA) elaboró unos principios de protección de datos que se aprobaron en 1996 como un estándar nacional, el *Model Code for the Protection of Personal Information*, por la *Standards Council of Canada*. Tras un debate sobre si respecto al sector privado debía regularse o limitarse a la autorregulación, se aprobó la *Personal Information Protection and Electronic Documents Act* (PIPEDA) que incorporó en su anexo 1 el código mencionado, *Principles set out in the national standard of Canada entitled Model code for the protection of personal information, CAN/CSA-Q830-96*. El primero de los principios incluidos en este código es el de *accountability: "An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles", Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c. 5, Anexo 1, 4.1, http://laws-lois.justice.gc.ca/PDF/p-8.6.pdf, (fecha consulta: 2.8.2014). Para más información ver: N. HOLMES, *Canada's Federal Privacy Laws*, PRB 07-44E, *Law and government division, revised 25 September 2008*, http://www.parl.gc.ca/Content/LOP/researchpublications/prb0744-f.htm (fecha consulta: 5.8.2014).

[1584] Se establece el principio de *accountability* denominado responsabilidad en el artículo 6: "Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley." El enunciado del principio se recoge en el artículo 14: "El responsable velará por el cumplimiento de

En lo que respecta a las legislaciones nacionales europeas se contemplan algunos rasgos del principio[1585]. Así, por ejemplo, el RLOPD también se podría considerar que incorpora un deber de *accountability*, en lo que se refiere a las medidas de seguridad que deben cumplir el responsable y el encargado del tratamiento. Así, esta norma obliga a que se adopte un catálogo de medidas que incluyen la elaboración de un documento de seguridad. No obstante, el enfoque no es exactamente el del principio de *accountability* al carecer de la flexibilidad que entiendo es una característica que define a este sistema, como se examinará más adelante. En consecuencia, entiendo que en el RLOPD prima la rigidez de la regulación sobre la autorregulación.

En la Propuesta de Madrid se incluía el principio de *accountability* denominado en este texto "de responsabilidad". El principio establece que "la persona responsable deberá: a) adoptar las medidas necesarias para cumplir con los principios y obligaciones establecidos en el presente documento y en la legislación nacional aplicable, y b) dotarse de aquellos mecanismos necesarios para evidenciar dicho cumplimiento, tanto ante los interesados como ante las autoridades de supervision en el ejercicio de sus competencias, conforme a lo establecido en el apartado 23" (apdo. 11 Propuesta de Madrid). A la formulación del principio se añadía la alusión a unas "medidas proactivas" que son medidas típicas de la *accountability* (apdo. 22 Propuesta de Madrid). Los Estados debían incentivar el establecimiento de estas medidas por parte de los responsables para cumplir la legislación en materia de protección de datos.

En lo que respecta a estándares, la *International Organization for Standardization* (ISO) y la *International Electrotechnical Commission* (IEC), que conforman la organización internacional líder en materia de estandarización también han incluido este

---

los principios de protección de datos personales establecidos por esta Ley, debiendo adoptar las medidas necesarias para su aplicación. Lo anterior aplicará aún y cuando estos datos fueren tratados por un tercero a solicitud del responsable. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.", ambos preceptos en la Ley federal de protección de datos personales en posesión de los particulares, 5.7.2010, http://inicio.ifai.org.mx/LFPDPPP/LFPDPPP.pdf (fecha consulta: 5.8.2014) (Ley mexicana). Además el principio se desarrolla en los artículos 47 y 48 del Reglamento de la ley federal (México) de protección de datos personales en posesión de los particulares, 21.12.2011, http://inicio.ifai.org.mx/PROTECCIONDEDATOSPERSONALES/RLFPDPP.pdf (fecha consulta: 5.8.2014) (Reglamento de desarrollo de la Ley mexicana).

[1585]Así se pudo ver en el Capítulo V, como algunas leyes nacionales europeas obligaban a documentar las medidas de seguridad adoptadas o a realizar evaluaciones de riesgos (art. 13.2 Ley checa, art. 11 Ley islandesa).

principio en la norma ISO/IEC 29100:2011[1586]. Esta norma proporciona un marco de referencia para la protección de información personal identificable en sistemas de tecnología de la información y de las comunicaciones. Uno de los puntos que establece es el de *accountability*, cuyo enunciado es: "*The processing of PII [personally identifiable information] entails a duty of care and the adoption of concrete and practical measures for its protection*" (apdo. 5.10 ISO/IEC 29100:2011).

El GA29 también hace referencia al proyecto sobre *accountability* que lleva a cabo *The Centre for Information Policy Leadership Hunton&Williams LLP* (Proyecto sobre accountability*)*, que reúne a expertos provenientes de grandes compañías, agencias de protección de datos y académicos, que analizan los efectos que puede tener la aplicación de este principio en las empresas[1587]. Este proyecto, que se inició en el 2009, ha tenido hasta ahora cuatro fases en las que se han elaborado documentos con el resultado de los estudios.

En la primera fase, que se desarrolló en el 2009 y se denominó proyecto *Galway* (ya que tuvo un importante papel la autoridad de control irlandesa, el *Irish Data Protection Commissioner*), se definieron cinco elementos esenciales de la *accountability*, que tenían como objetivo ayudar a las organizaciones a medir si cumplían o no el principio[1588]. En la segunda fase, denominada proyecto París, que tuvo lugar en el 2010, se realizó un análisis de cómo las organizaciones demuestran la *accountability* y cómo las entidades reguladoras pueden medir la *accountability*[1589]. La tercera fase se refirió al debate surgido sobre si la *accountability*, para ser efectiva, debía ser requerida por el

[1586] ISO/IEC 29100:2011(E), *Joint Technical Committee* ISO/IEC JTC 1, *Information technology, Subcommittee SC 27, IT Security techniques*.

[1587] Dictamen 3/2010 sobre el principio de responsabilidad, *op. cit*., pág.7, nota al pie 3. Este proyecto ha reunido a algunas de las empresas más importantes (Intel, *Google*, Hewlett Packard, Oracle, Salesforce.com, IBM, Microsoft, Accenture, Symantec, Vodafone, Bank of America, Acxiom, Procter&Gamble, Intuit, Total, TRUSTe, Which?, Nokia, Merck&Co, Visa), autoridades de protección de datos de España, Francia, Italia, Irlanda, Canadá, Alemania, Hungría, Israel, Países Bajos, Reino Unido, Bélgica, Mexico, Estados Unidos, el Supervisor europeo, así como organizaciones dedicadas a la defensa del derecho a la protección de datos, la OCDE y personas de universidades como Fred Cate de la Universidad de Indiana o K. Krasnow Waterman del *Massachusetts Institute of Technology*. http://www.informationpolicycentre.com/resources/#accountability (fecha consulta: 2.8.2014).

[1588] Los resultados se reflejaron en el documento *Data protection accountability: the essential elements a document for discussion, October 2009, The Centre for Information Policy Leadership Hunton&Williams LLP*.

[1589] El documento resultante es *Demonstrating and measuring accountability a discussion document, Accountability Phase II-The Paris project, October 2010, The Centre for Information Policy Leadership Hunton&Williams LLP*.

mercado, tuvo lugar en el 2011 y se denominó proyecto Madrid, por celebrarse en la sede de la AEPD[1590]. La cuarta fase, que tuvo lugar en 2012, respondió a la necesidad de proporcionar una herramienta a las organizaciones para que pudieran aplicar y evaluar los programas necesarios para establecer un sistema de *accountability*[1591].

En cuanto a las reformas de los principales cuerpos normativos europeos en materia de protección de datos, también se ha incluido este principio en los textos que se barajan. Tanto en la reforma que se ha planteado del Convenio 108[1592], como en la PCE-RGPD, tal como veremos.

En EEUU, se ha incorporado el principio en el listado, que incluye la *Consumer Privacy Bill of Rights* presentada por el presidente Barack Obama en el año 2012[1593]. Asimismo, se ha incorporado en un borrador de ley, derivado de esta iniciativa y que se publicó en febrero de 2015 al que haré referencia posteriormente: la *Consumer Privacy Bill of Rights Act*[1594].

b. Las principales características del principio extraídas de los diferentes instrumentos jurídicos analizados

De la revisión de los textos mencionados, en los que se incluye el principio de *accountability*, se pueden extraer algunas características del principio. Sin embargo, hay

[1590] El documento resultante es *Implementing accountability in the marketplace a discussion document, Accountability phase III-The Madrid project, November 2011, The Centre for Information Policy Leadership Hunton&Williams LLP*.

[1591] Esta herramienta de autoevaluación, el *Self-assessment of a comprehensive privacy programme: a tool for practitioners,* tomó como punto de partida el documento "*Getting Accountability Right with a Privacy Management Program,*" desarrollado por autoridades de control de Canadá (*Federal Privacy Commissioner of Canada, Information Commissioners of Alberta and British Columbia).*

[1592] Si bien no se incluye expresamente como tal principio, sino que se encuentra recogido, por el momento, en el artículo 8 bis, titulado "obligaciones adicionales", que establece "1. *Each party shall provide that controllers and, where applicable, processors, shall take all appropiate measures to comply with the obligations of this Convention and be able to demonstrate, in particular to the competent supervisory authority provided for in Article 12 bis, that the data processing under their control is in compliance with the provisions of this Convention*". *Abridged report of the 3rd and final meeting (Strasbourg, 1-3 December 2014), CM(2015)40, Ad hoc Committe on Data Protection (CAHDATA), Council of Europe, Strasbourg, 3 March 2015.*

[1593] Ver Capítulo I. En esta lista de principios se encuentra el de *accountability: "Consumers have a right to have personal data handled by companies with appropiate measures in place to assure they adhere to the Consumer Privacy Bill of Rights*."

[1594]*Consumer Privacy Bill of Rights Act of 2015*, publicada el 27.2.2015, https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf (fecha consulta: 12.3.2015).

que matizar previamente que, si bien el enunciado del principio parece haber adquirido más o menos unanimidad en los textos, no así su desarrollo. De esta forma, en los diferentes textos se observa gran diversidad en lo que se considera que debería ser el contenido del principio. En algunos casos, se solapa con otros principios, como el de seguridad o la regulación de transferencias internacionales.

Lo primero que debe señalarse es que el principio de *accountability* no supone una modificación de las obligaciones preexistentes que tiene el responsable[1595]. De esta forma, podríamos decir que este principio genera obligaciones adicionales, de carácter más formal, que se añaden a las obligaciones de carácter material, correspondientes a los principios y derechos enunciados en la legislación. La *accountability* no es más que una formalización de una obligación, que ya antes de su incorporación a la norma, debía cumplir el responsable. El responsable, para poder cumplir con lo previsto en la legislación debía instaurar unas medidas en su organización. Ahora lo que se hace es convertir esta obligación, que antes era implícita, en una obligación explícita.

Otra característica que resaltaré de este principio es que la *accountability* reside en la organización responsable del tratamiento, que es la que debe cumplir con las obligaciones que se deriven de la normativa de protección de datos[1596]. Esto implica que aunque el responsable contrate a otro sujeto para llevar a cabo el tratamiento (el encargado del tratamiento) también seguirá siendo responsable, en materia de *accountability*[1597].

[1595] *Data protection accountability: the essential elements a document for discussion, October 2009, The Centre for Information Policy Leadership Hunton&Williams LLP,* pág.9.

[1596] Así el artículo 6 de la Ley canadiense establece, de forma expresa, que la designación de personas para cumplir con la *accountability,* no implica que la organización no deba cumplir con lo establecido en el código de conducta anexado a la ley. La Ley canadiense no ha creado la figura del responsable del tratamiento, de forma que no hay concepto y se refiere a la organización como la obligada a cumplir con los preceptos de la norma. En el código de conducta anexado se incluye el principio de *accountability* que deja claro que la organización es responsable por la información personal bajo su control (punto 4.1 Anexo 1 Ley canadiense).

[1597] La legislación mexicana especifica que "el responsable tiene la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, o por aquéllos que haya comunicado a un encargado, ya sea que este último se encuentre o no en territorio mexicano." (art. 47 Reglamento de desarrollo ley mexicana). La Ley canadiense así lo establece y además indica que la organización responsable deberá utilizar medios, como los contratos, para asegurarse de que el tercero contratado proteja la información (punto 4.1.3 Anexo 1 Ley canadiense). La Guía OCDE 2013 establece que el programa de gestión de la privacidad debe cumplir con lo establecido en la Guía OCDE respecto a los datos personales bajo el control del responsable (15.a.i Guía OCDE 2013). En este sentido, el hecho de referirse a datos "bajo el control" refleja que el programa debe incluir no sólo las operaciones que lleva a cabo el responsable, sino también aquellas de las que pueda ser responsable, como por ejemplo, las que

Sin embargo, al mismo tiempo, otra característica del sistema de *accountability* es que exige la necesidad de implicar a personas concretas, en el cumplimiento de las medidas, así como, especialmente, a la dirección de la organización[1598].

Otra característica es lo que se definiría como el contenido principal de la obligación, es decir, en lo que se traduce la misma. Este contenido consistiría en la adopción de políticas y de medidas para aplicar estas políticas. Las políticas serían aquellos documentos adoptados por la dirección de la organización que expresarán la estrategia a adoptar en la materia de una forma general. Las medidas para aplicar las políticas serían los procedimientos, que deberían ponerse en funcionamiento para hacer efectivas las políticas, de forma que serían la concreción de estas. Estos procedimientos incluirán medidas determinadas que será preciso implementar.

En algunos casos, se observa que se realiza un simple enunciado de esta obligación, lo que daría mayor margen de maniobra para el responsable en la elección de

---

lleven a cabo agentes por su cuenta. Además en este texto, esto también implica que se deban tener en cuenta medidas, en caso de corresponsabilidad. Se indica en el informe adicional explicativo de la nueva versión de la guía que estas medidas pueden ser estipulaciones contractuales, que obliguen a cumplir con las políticas de privacidad del responsable, protocolos de notificación de incidencias, formación del personal, regulación de subcontrataciones y el establecimiento de auditorías. *Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013)*.

[1598] La Ley canadiense es ejemplo de la plasmación de esta necesaria designación de personas concretas, ya que establece que la organización responsable designe una persona o personas que se hagan responsables del cumplimiento de los principios para la protección de la información, enunciados en el anexo 1 (Anexo 1, punto 4.1 Ley canadiense,). También se establece que participen otras personas en quienes la persona designada puede delegar (Anexo 1, punto 4.1.1 Ley canadiense). Además debe identificarse a la persona designada cuando se solicite (Anexo 1, punto 4.1.2 Ley canadiense). Otros ejemplos son la Propuesta de Madrid que también establece la designación de uno o varios oficiales de privacidad o de protección de datos, con cualificación, recursos y competencias suficientes para ejercer adecuadamente sus funciones de supervisión (art. 22.b Propuesta de Madrid) y la norma ISO/IEC 29100:2011 que especifica la designación de una persona en la organización, para que se encargue de aplicar las políticas, procedimientos y prácticas para proteger la privacidad que además podrá delegar en otras (apdo. 5.10 ISO/IEC 29100:2011). La asignación de recursos a las personas encargadas de cumplir con las obligaciones se establece, por ejemplo, en el Proyecto sobre accountability como un aspecto fundamental que debe reunir un programa de *accountability*. *Demonstrating and measuring accountability a discussion document, Accountability Phase II-The Paris project, October 2010, The Centre for Information Policy Leadership Hunton&Williams LLP*, pág. 6. En lo que se refiere a la implicación de la dirección de la organización responsable en la *accountability*, un ejemplo se halla en la Guía OCDE 2013, que especifica que el programa de gestión de la privacidad debe integrarse en la estructura de gobierno (15.a.iv Guía OCDE 2013). En el Proyecto sobre accountability, entre los cinco elementos esenciales que se identifican en la primera fase, en el denominado proyecto de *Galway*, está el primero que es "compromiso de la organización con la *accountability*" (*organisation commitment to accountability*). Para profundizar en el contenido de este elemento ver *Data protection accountability: the essential elements a document for discussion, October 2009, The Centre for Information Policy Leadership Hunton&Williams LLP*, págs. 11 a 12.

las medidas concretas a adoptar. Sin embargo, en otros, especialmente en las legislaciones, se introducen medidas concretas que no creo respeten la esencia del principio, que lo que pretende es que sea el responsable el que decida cómo aplicarlo y lo ajuste en función del riesgo. La flexibilidad que el sistema otorga al responsable para adoptar estas medidas es sin duda una cuestión controvertida, como se verá en la aproximación a la reforma de la Directiva 95/46/CE[1599].

Ejemplos de las medidas a adoptar se encuentran en la Ley canadiense que enumera algunas de forma no exhaustiva: procedimientos para proteger la información, procedimientos para recibir y responder reclamaciones y solicitudes, formación del personal y comunicación de políticas y prácticas al mismo, desarrollo de información para explicar las políticas y procedimientos de la organización (punto 4.1.4, Anexo 1 Ley canadiense). Asimismo, en el Proyecto sobre *accountability,* entre los cinco elementos esenciales que se identifican en la primera fase, en el denominado proyecto de *Galway*, está en el primero "la adopción de políticas internas coherentes con criterios externos"[1600]

[1599] Esta flexibilidad se contempla claramente en la Guía OCDE 2013, que indica que el programa de gestión de la privacidad debe dotarse de flexibilidad y adaptarse a la estructura, escala, volumen y sensibilidad de las operaciones (15.a.ii Guía OCDE 2013) y debe incluir medidas adecuadas en función de la evaluación de riesgos de la privacidad (*privacy risk assessment*) (15.a.iii Guía OCDE 2013). Por tanto, se trata de que los programas se establezcan en función de lo crítico que sea el tratamiento de datos personales y de la estructura del responsable. El informe adicional de la nueva versión de la guía indica que, en la puesta en marcha de este tipo de programas, debe atenderse a la estructura del responsable, por ejemplo, si tiene muchas ubicaciones en múltiples jurisdicciones debe considerar mecanismos de supervisión diferentes a los que puede contemplar un responsable de tamaño pequeño o medio, que sólo cuente con un establecimiento. Asimismo, el informe se refiere a la necesidad de ajustar el programa a la sensibilidad del tratamiento que lleve a cabo el responsable o al volumen de los datos. De esta forma, se huye del catálogo de medidas a adoptar de forma objetiva y se persigue la eficiencia. *Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013).* El catálogo de medidas de seguridad que establece la normativa española en el RLOPD sería un ejemplo de este enfoque que se estaría dejando atrás.

[1600] Traducción de la autora de "*adoption of internal policies consistent with external criteria"*. Es interesante la alusión del primer elemento esencial del Proyecto sobre *accountability* a los criterios externos a los que debe acudir el responsable, cuando adopte sus política internas. Este proyecto no se centra en un determinado marco legislativo, sino que desarrolla el principio de *accountability* desde una perspectiva autónoma. Por ello, lo que se pretende es que el responsable acuda a la fuente pertinente, la legislación que le sea aplicable o a principios generalmente aceptados o buenas prácticas del sector. Este extremo es coherente con el espíritu de compromiso que inspira este principio que, como se ha indicado responde a que el responsable se autoimponga un determinado nivel de protección de los datos personales, con el fin de asegurar una uniformidad en su organización, sin tener que preocuparse de aplicar en cada territorio una normativa distinta. En este mismo sentido, el Reglamento de desarrollo de la Ley mexicana indica que el responsable, para cumplir con la obligación de responsabilidad "podrá valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que determine adecuado para tales fines" (art. 47 Reglamento de desarrollo de la Ley mexicana). No obstante, también se incluye un listado de las medidas que, como mínimo, el responsable debe adoptar (art. 48 Reglamento de desarrollo de la Ley mexicana).

y en el segundo "mecanismos para aplicar las políticas, incluyendo herramientas, formación y educación"[1601].

La formación y capacitación del personal es una medida que se contempla en algunos textos de forma expresa, aunque de nuevo estamos ante una medida que es evidente que el responsable debe adoptar. Así, por ejemplo, se incluye en la Propuesta de Madrid[1602], en la norma ISO/IEC 29100:2011[1603] y, si bien no se contempla entre los elementos esenciales que recoge el Proyecto sobre *accountability* sí se considera un elemento que debe cumplir el responsable y que le servirá para demostrar que es *accountable*[1604].

También se han incorporado como medidas en la Propuesta de Madrid buenas prácticas, como son la privacidad en el diseño (*privacy by design*)[1605], las evaluaciones de impacto sobre protección de datos (*privacy impact assessement*), que tienen como finalidad formalizar el análisis, que forzosamente debe realizar el responsable ante la puesta en marcha de un tratamiento de datos para poder valorar las medidas a adoptar[1606] y la implementación de planes de contingencias que establezcan unas pautas de actuación, en caso de que se verifique un incumplimiento de la legislación[1607].

[1601] Traducción de la autora de "*mechanisms to put privacy policies into effect, including tools, training and education*". Para profundizar en el contenido de este elemento ver *Data protection accountability: the essential elements a document for discussion, October 2009, The Centre for Information Policy Leadership Hunton&Williams LLP,* págs. 11 a 12.

[1602] "La realización periódica de programas de concienciación, educación y formación entre los miembros de la organización destinados al mejor conocimiento de lalegislación que resulte aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal, así como de los procedimientos establecidos por la organización a tal efecto." (art. 22.c) Propuesta de Madrid).

[1603] Establece la necesidad de que se realice una formación adecuada al personal del responsable que acceda a los datos personales, (5.10 ISO/IEC 29100:2011).

[1604] Así entre estos elementos que se consideran fundamentales en la implementación de un programa de *accountability*, está la educación y formación para empleados y subcontratistas. *Demonstrating and measuring accountability a discussion document, Accountability Phase II-The Paris project, October 2010, The Centre for Information Policy Leadership Hunton&Williams LLP,* pág. 6.

[1605] Así se define como "la adaptación de aquellos sistemas y/o tecnologías de información destinados al tratamiento de datos de carácter personal a la legislación que resulte aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal, en particular al decidir acerca de sus especificaciones técnicas y en su desarrollo e implementación." (art. 22.e) Propuesta de Madrid).

[1606] Esta medida se describe como "la puesta en práctica de estudios de impacto sobre la privacidad previos a la implantación de nuevos sistemas y/o tecnologías de información destinados al tratamiento de datos de carácter personal, así como a la puesta en práctica de nuevas modalidades de tratamiento de datos de carácter personal o a la realización de modificaciones sustanciales en tratamientos ya existentes." (art. 22.g) Propuesta de Madrid).

[1607] Artículo 22.h) Propuesta de Madrid.

Otra característica que quiero resaltar de los sistemas de *accountability* es la adopción de sistemas de seguimiento y verificación de que se cumplen las políticas y medidas proyectadas. De nuevo, es importante que se establezcan estos mecanismos porque es esencial que además de aplicar las medidas, el responsable se asegure de que se cumplen, en todo momento y de que son eficaces. Ello es imprescindible en un contexto cambiante como el tecnológico, en el que las medidas se pueden volver obsoletas en un corto período de tiempo[1608].

Una característica que forma parte, habitualmente, del enunciado general es la necesidad de que el responsable, además de adoptar todas estas medidas, sea capaz de demostrar que las ha adoptado. Esta capacidad de probar se traduce necesariamente en una obligación de documentar las medidas que adopta, lo que permitirá que se pueda medir el grado de cumplimiento del responsable[1609].

Pero ¿ante quién debe demostrar el responsable que cumple con el principio? El Proyecto sobre *accountability* señala tres colectivos: los titulares de los datos, las autoridades de protección de datos y los colaboradores comerciales. Y es que un interesante aspecto que también analiza este proyecto es el de la adopción de sistemas de *accountability* fruto de que lo requiera el propio mercado[1610]. En la Guía de la OCDE 2013 se establece la necesidad de que el responsable esté preparado para demostrar que el

[1608] De esta forma, entre los cinco elementos esenciales que se identifican en el Proyecto sobre *accountability* está el tercero que hace referencia a los sistemas de revisiones internas y verificaciones externas (*systems for internal, ongoing oversight and assurance reviews and external verification*). Asimismo, el programa de gestión de la privacidad de la Guía OCDE 2013 debe incluir mecanismos de supervisión interna, así como debe actualizarse en virtud de la revisión continua y los análisis periódicos (15.a.iv y 15.a.iii Guía OCDE 2013). También la Propuesta de Madrid contempla la realización de auditorías (art. 22.d) Propuesta de Madrid).

[1609] De esta forma, el Proyecto sobre *accountability* dedicó una de sus fases precisamente al estudio de la demostración y de la métrica de la *accountability*. Fruto de este estudio se enumeran nueve fundamentos que se considera que el responsable debe cumplir para poder demostrar que cumple con el principio: 1. Políticas, 2. Supervisión ejecutiva, 3. Dotación de personal y delegación, 4. Educación y formación, 5. Evaluación continua de riesgos y mitigación, 6. Programa de evaluación de riesgos y validación, 7. Gestión de incidencias y de reclamaciones, 8. Cumplimiento interno, 9. Compensación. Ver para más información el documento: *Demonstrating and measuring accountability a discussion document, Accountability Phase II-The Paris project, October 2010, The Centre for Information Policy Leadership Hunton&Williams LLP*. La norma ISO/IEC 29100:2011 cuando define lo que significa *accountability* ya presupone la adopción de políticas, procedimientos y prácticas para proteger la privacidad y en lo que incide es en el hecho de que deben documentarse y comunicarse (5.10 ISO/IEC 29100:2011).

[1610] *Implementing accountability in the marketplace a discussion document, Accountability phase III-The Madrid project, November 2011, The Centre for Information Policy Leadership Hunton&Williams LLP*. En no pocas ocasiones las empresas adoptan estos sistemas forzados por sus clientes que exigen que se cumplan para evitar posibles repercusiones en su reputación o incluso una posible responsabilidad por incumplimiento del subcontratista. Si unas organizaciones obligan a otras se crea un contagio en la adopción de estos mecanismos.

programa de gestión de la privacidad es apropiado, especialmente si se lo solicita una autoridad de control de protección de datos y otra entidad responsable de controlar el cumplimiento de un código de conducta u otras herramientas que obliguen a la aplicación de la guía[1611].

Otra característica sería la transparencia y los procedimientos para atender reclamaciones[1612]. Lo que se persigue es contribuir a otorgar al titular de los datos la capacidad de control sobre estos y evitar la opacidad del sistema adoptado. Esto comporta abrir canales de comunicación con estos titulares de datos, de forma que puedan solicitar información o interponer reclamaciones. Asimismo, esta característica se refleja en la obligación de notificar los fallos de seguridad que puedan producirse y que afecten a los datos[1613].

[1611] 15.b Guía OCDE 2013. Como ejemplos de estos instrumentos se citan esquemas de certificación, sellos y también reglas como las *Binding Corporate Rules* (BCRs) europeas o el Sistema de reglas para realizar transferencias de la APEC. *Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013)*.

[1612] Entre los cinco elementos esenciales que se identifican en el Proyecto sobre *accountability* está el cuarto consistente en "transparencia y mecanismos de participación"(*transparency and mechanisms for individual participation*) y el quinto que es "medios para reclamación y medidas coercitivas externas"(*means for remediation and external enforcement*). En la Ley canadiense el principio 10 se refiere al derecho a reclamar por el no respeto de los principios enunciados en la ley, entre los que se incluye la obligación de que las organizaciones establezcan procedimientos para recibir reclamaciones y solicitudes de información (punto 4.10, Anexo 1 Ley canadiense). En la Guía OCDE 2013 el programa de gestión de la privacidad debe incluir planes para atender solicitudes de información e incidentes (15.a.v Guía OCDE 2013). La norma ISO/IEC 29100:2011 establece la necesidad de que existan procesos de gestión de reclamaciones y de compensación que puedan utilizar los titulares de los datos. Resalta esta norma que los procedimientos para perseguir la compensación son importantes en un sistema de *accountability* ya que permiten que el titular de los datos pueda exigir la responsabilidad por un mal uso y hace que aumente la confianza en mantener una relación con el responsable. En la Propuesta de Madrid también se cita, entre las medidas a adoptar por el responsable, la de establecer procedimientos destinados a prevenir y detectar infracciones, que podrán basarse en modelos estandarizados de gobierno y/o gestión de la seguridad de la información (art 22.a) Propuesta de Madrid).

[1613] En la Guía OCDE 2013 se obliga al responsable a notificar los fallos de seguridad que afecten a datos personales a las autoridades de control de protección de datos u otras autoridades competentes, así como a los concretos afectados si el incidente de seguridad les pudiera afectar negativamente (15.c Guía OCDE 2013). También la norma ISO/IEC 29100:2011 establece que se informe a los titulares de los datos de los incidentes que les puedan ocasionar un daño sustancial así como las medidas para resolverlos, excepto si esto está prohibido y también indica que debe informarse a todos los interesados (*stakeholders*) en violaciones de datos (por ejemplo a las autoridades de control) dependiendo del nivel de riesgo (5.10 ISO/IEC 29100:2011).

c. El desarrollo del principio en el proyecto de reglamento

i. Diversos enfoques en la formulación del principio en los textos preparatorios

Los enfoques de las tres instituciones, Comisión, Parlamento y Consejo UE, durante el proceso legislativo contemplan importantes diferencias en la aproximación al principio de *accountability*, desde su reconocimiento como principio, hasta su desarrollo.

(1) El enfoque de la Comisión Europea

La Comisión lo incluyó, tal como había sugerido el GA29, en su propuesta como uno de los principios relativos al tratamiento de datos personales y establecía que los datos personales deberían ser "tratados bajo la responsabilidad del responsable del tratamiento, que, para cada operación del tratamiento, garantizará y demostrará el cumplimiento de las disposiciones del presente Reglamento" (art. 5.f) PCE-RGPD)[1614]. Por tanto, se puede decir que el principio irrumpió con fuerza en la construcción del nuevo marco jurídico del derecho a la protección de datos.

Respecto al desarrollo del principio, la Comisión estableció que el responsable debía adoptar políticas e implementar medidas para asegurar y poder demostrar que el tratamiento se lleva a cabo de conformidad con el reglamento, así como mecanismos para verificar la eficacia de las medidas adoptadas, como auditorías (art. 22.1 y .3 PCE-RGPD). La Comisión incluyó un listado no exhaustivo y mínimo de las medidas que el responsable debería adoptar: conservación de documentación, cumplir los requisitos en materia de seguridad, realizar una evaluación de impacto, cumplir los requisitos en materia de autorización o consulta previas de la autoridad de control y designación de un

[1614]El principio se introdujo desde el primer momento, en el primer borrador hecho público por la Comisión: *"Personal data must be: processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation"* (art. 4.1.f) PCE-RGPD No oficial). El enunciado del principio recoge los dos elementos esenciales que perfilaba el GA29 en su dictamen como parte del principio general de *accountability*: la obligación de cumplir el Reglamento y la capacidad de demostrar este cumplimiento o rendición de cuentas. El GA29 proponía la inclusión del siguiente precepto: «Artículo X – Aplicación de los principios de protección de datos. 1. El responsable del tratamiento de datos aplicará medidas adecuadas y eficaces para garantizar el cumplimiento de los principios y obligaciones dispuestos en la Directiva. 2 A instancias de la autoridad de control, el responsable del tratamiento de datos demostrará el cumplimiento del apartado 1.». Dictamen 3/2010, sobre el principio de responsabilidad, *op. cit.*, pág. 10.

delegado de protección de datos (art. 22.2 PCE-RGPD)[1615]. Estas medidas mínimas correspondían con algunas de las obligaciones establecidas en el estatuto y podrían ser ampliadas por la Comisión, entre otras cosas, para adaptarlas a las pequeñas y medianas empresas y las microempresas (pymes y micropymes) (art. 22.4 PCE-RGPD).

(2) El enfoque del Parlamento Europeo

El Parlamento confirmó su reconocimiento, como tal principio e incluyó la referencia expresa al mismo como "principio de rendición de cuentas" o, en la versión en inglés, "*accountability*". De acuerdo con el texto modificado por el Parlamento, este principio implica que los datos personales serán "tratados bajo la responsabilidad del responsable del tratamiento, que garantizará y será capaz de demostrar el cumplimiento de las disposiciones del presente Reglamento (rendición de cuentas)" (art. 5.f) PPE-RGPD).

Asimismo, mantuvo, en su desarrollo, la obligación del responsable de adoptar políticas y aplicar medidas técnicas y organizativas apropiadas y verificables, que aseguraran y demostraran, de forma transparente, que el tratamiento se llevaba a cabo, de conformidad con el reglamento (art. 22.1. PPE-RGPD).

Se introdujo en este trámite parlamentario un componente de flexibilidad que no estaba en el texto de la Comisión, al incluir que en la puesta en marcha de estas políticas y medidas, se debían tener en cuenta las técnicas existentes, la naturaleza de tratamiento de los datos personales, el contexto, el alcance y los fines del tratamiento, los riesgos para los derechos y libertades de los interesados, y el tipo de organización[1616], y ello, tanto en

[1615] En lo referente al desarrollo del principio, el GA29 propuso dos opciones: no desarrollarlo, sino incluir en la nueva norma el principio general sin más, de forma que se diera más libertad a los responsables en la elección de las medidas concretas que deberían adoptar para cumplirlo o establecer el principio general y añadir una lista no exhaustiva de medidas, a modo de caja de herramientas para responsables, que se pudieran fomentar a nivel nacional. El GA29 además citaba como ejemplo de texto en el que se había incorporado este listado de medidas la Propuesta de Madrid y proponía ya un listado de medidas a modo ejemplificativo. En su propuesta, el GA29, consciente de la posible incerteza que podría originar esta falta de concreción, sugería que fuera el mismo grupo, las autoridades de control o la Comisión Europea, las que dieran pautas a los responsables en la adopción de estas medidas. *Ibídem*.

[1616] El GA29 se había referido a la modulación de las medidas, de forma que recalcaba que las medidas a adoptar debían adaptarse en cada caso concreto al riesgo del tratamiento de datos y a la naturaleza de los datos, tal como se había establecido en el artículo 17 Directiva 95/46/CE en materia de seguridad. De esta forma precisaba que podían haber responsables de tratamiento pequeños que, no obstante, trabajaran con

el momento de determinar los medios del tratamiento, como en el momento del tratamiento propiamente dicho[1617].

Uno de los fines del principio de *accountability* es eliminar cargas administrativas para los responsables. Por ello, se debatió en el proceso parlamentario si debía introducirse entre los elementos de flexibilidad el tamaño de la empresa, lo que perseguía suavizar las exigencias para las pymes y micropymes. Finalmente, se optó por aludir al tipo de organización y no al tamaño de la organización, que, si bien es más neutro, parece mantener esta intención de admitir menores exigencias para las empresas pequeñas[1618]. No obstante, se puede advertir en el proceso de elaboración del reglamento un tira y afloja en lo que respecta al hecho de relajar los requisitos para pymes y micropymes. Así, se eliminó el artículo 22.4 PCE-RGPD que permitía a la Comisión Europea la adopción de medidas específicas para este tipo de empresas[1619].

---

datos que originaran un alto riesgo para los interesados. Dictamen 3/2010, sobre el principio de responsabilidad, *op. cit.*, pág. 14.

[1617] La enmienda 1660 de Nils Torvalds al artículo 22.1 además de incluir los elementos de flexibilidad (es decir que al adoptar las medidas se tengan en cuenta los datos personales, el tipo de organización, las técnicas existentes) extendía la obligación, tanto al momento de determinación de los medios, como en el tratamiento propiamente dicho. Asimismo en la enmienda se proponía aludir a la implementación de programas de privacidad que garantizaran el cumplimiento de los requisitos del reglamento y la protección de los derechos del interesado desde el diseño. No obstante, finalmente no se incluyó en el texto esta alusión a la protección desde el diseño, aunque sí se conservó la referencia a todo el ciclo del tratamiento. Enmiendas (5), 1493 – 1828, Proyecto de informe Jan Philipp Albrecht (PE501.927v04-00) sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) Propuesta de Reglamento, (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 6.3.2013.

[1618] Así la enmienda 1662 de Salvatore Iacolino que recogía el proyecto de informe del ponente proponía añadir al artículo 22.1 que "dichas medidas serán proporcionales al tamaño del responsable del tratamiento, la naturaleza de los datos tratados y la repercusión del tratamiento para los interesados", lo que se justificaba con el objetivo de confirmar la importancia del principio de responsabilidad de las empresas pero sin crear cargas administrativas excesivas, en particular para las PYMES. Enmiendas (5), 1493 – 1828, Proyecto de informe Jan Philipp Albrecht (PE501.927v04-00) sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) Propuesta de Reglamento, (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 6.3.2013.

[1619] Enmiendas 1699 a 1704 que proponen la supresión de este apartado por innecesario. Enmiendas (5) 1493 – 1828, Proyecto de informe Jan Philipp Albrecht (PE501.927v04-00) sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) Propuesta de Reglamento, (COM(2012)0011–C7-0025/2012 – 2012/0011(COD)), 6.3.2013. Asimismo, en el dictamen, mediante el que el GA29 proporcionaba más orientaciones para el debate sobre el proyecto del Reglamento, incluía sus comentarios acerca de la primera versión de la norma respecto a aquellas disposiciones que contemplaban un desarrollo mediante actos delegados de la Comisión Europea. El GA29 realizó un comentario sobre el artículo 22.4 PCE-RGPD, que no consideraba apropiado, ya que estimaba que el desarrollo de las medidas debía quedar, en manos del propio responsable. El GA29 manifestaba que no debían haber excepciones en la aplicación del principio de *accountability*, independientemente de la dimensión del responsable del tratamiento. No obstante, sí que consideraba admisible que las microempresas adaptaran las medidas a su escala. Dictamen 8/2012 por el que se

El texto parlamentario incluyó la obligación de adoptar "las medidas razonables para aplicar políticas y procedimientos de control del cumplimiento que respeten sistemáticamente las decisiones autónomas de los interesados" (art. 22.1bis PPE-RGPD). Estas políticas debían revisarse cada dos años y actualizarse cuando fuera necesario. Por tanto, en este nuevo apartado se hace referencia claramente al control del cumplimiento *a posteriori* que debe llevar a cabo el responsable. Sin embargo, la mención al respeto sistemático de las decisiones autónomas de los interesados resulta algo confusa.

El Parlamento cambió de lugar el requisito relativo a la necesaria verificación de la eficacia de las medidas adoptadas mediante auditorías, que había incluido la Comisión, de forma que lo trasladó a la parte del preámbulo (Considerando 60 PPE-RGPD). Si bien podría parecer que esto suaviza la exigencia de este requisito, el tono del Considerando es taxativo: "esto debe ser verificado por auditores independientes internos o externos".

El texto del Parlamento estableció la obligación del responsable de "poder demostrar la idoneidad y eficacia de las medidas" (art. 22.3 PPE-RGPD). Por tanto, se refiere a la obligación de demostrar que cumple con las medidas proyectadas y que estas son idóneas, se entiende que para cumplir con el reglamento. En este sentido, se añadió una obligación de incluir en los informes periódicos del responsable una descripción de las políticas y medidas adoptadas, aunque se excluían las de control de cumplimiento. Esta obligación de inclusión en los informes ayudaría a la transparencia del cumplimiento del principio, de cara a las instituciones que supervisen a los responsables, o de cara a los interesados si se trata de informes que deben publicarse[1620].

Por último, el Parlamento eliminó el desglose de las medidas mínimas que debía adoptar el responsable. Estas medidas, como ya se ha indicado, eran parte de las obligaciones que se establecen en el estatuto del responsable. Por tanto, son obligaciones que debe adoptar, en todo caso, el mismo. Independientemente de que estas medidas puedan considerarse derivadas del principio de *accountability* o inspiradas por el mismo,

---

proporciona más información sobre los debates relativos a la reforma de la protección de datos, 01574/12/ES WP 199, de 5.10.2012, Grupo de trabajo Artículo 29 sobre la protección de datos, págs. 25 a 26.

[1620] Así se citan, como ejemplo, de este tipo de informes periódicos los informes obligatorios de las sociedades de cotización oficial.

resulta confuso que se integraran como parte de la *accountability*, cuyo objetivo, en el reglamento, debe orientarse a incorporar políticas y medidas para cumplir con las obligaciones establecidas.

(3) El enfoque del Consejo de la Unión Europea

El Consejo UE abandonó la consideración de la *accountability* como principio, y lo sustituyó por el texto que se incluía en la Directiva 95/46/CE, en los principios de calidad (art. 6.2 Directiva 95/46/CE), en el que se limitaba a indicar que el responsable debía cumplir con los mismos (art. 5.2 PCJ-RGPD). Sin embargo, mantuvo el precepto que desarrollaba el principio en el apartado dedicado al responsable del tratamiento (art. 22 PCJ-RGPD). No obstante, la obligación, de nuevo, diverge de los enfoques adoptados por la Comisión y el Parlamento.

El responsable deberá aplicar las medidas apropiadas y demostrar que el tratamiento de datos personales se lleva a cabo, de conformidad con el reglamento (art. 22.1 PCJ-RGPD). La adopción de políticas sólo es necesaria si se considera proporcionado a las actividades del tratamiento (art. 22.2bis PCJ-RGPD)[1621].

El Consejo UE también incluyó un componente de flexibilidad, en la línea del introducido por el Parlamento, a la hora de la adopción de las medidas, de forma que el responsable tendrá en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como la probabilidad y gravedad del riesgo para los derechos y libertades de las personas físicas.

Por último, el Consejo UE eliminó el listado de medidas mínimas, las referencias a los mecanismos de verificación de la eficacia de las medidas y la posibilidad de que la Comisión estableciera medidas adicionales. Sin embargo, el Consejo UE añadió la posibilidad para el responsable de utilizar la adhesión a códigos de conducta o las certificaciones para demostrar el cumplimiento de sus obligaciones (art. 22.2ter PCJ-RGPD).

1621

Por tanto, el Consejo UE incentiva la autorregulación por parte del responsable y minimiza, en consecuencia, la regulación que sólo obliga a instaurar medidas apropiadas pero deja la elección de las mismas al responsable. Ahora bien, entiendo que la adopción de políticas debería ser obligatoria, ya que son las políticas las que deben establecer la estrategia del responsable a seguir para la adopción de las medidas concretas.

ii. Las características del principio en el reglamento

Si recorremos las características extraídas de los diversos instrumentos jurídicos examinados, en los que se incluyen regulaciones sobre el principio de *accountability*, y acudimos al reglamento, vemos que se cumple prácticamente con todas, a lo largo de su regulación.

En primer lugar, tal como se extraía de los instrumentos jurídicos analizados, en el reglamento, la obligación derivada del principio de *accountability* lo que hace es añadirse a las otras que tiene el responsable fruto de la regulación y lo que persigue es el reforzamiento de las mismas[1622]. También se cumpliría con la característica de que la *accountability* reside en la organización que es responsable del tratamiento y se aplicaría a todos los responsables, independientemente de si pertenecen al sector público o privado[1623].

Con la designación del delegado de protección de datos se cumpliría, en parte, la característica señalada sobre la necesidad de implicar a personas concretas en el cumplimiento de las medidas. No obstante, como se verá cuando se aborde esta designación, el Consejo UE ha establecido que serán los Estados miembros quienes determinarán si debe imponerse o no la obligación de designarlo. También puede considerarse que se cumple con esta involucración de personas concretas, cuando el

[1622] Así lo planteaba el GA29. Dictamen 3/2010, sobre el principio de responsabilidad, *op. cit*., pág. 6.
[1623] El GA29 planteaba varios niveles en la arquitectura jurídica del sistema de responsabilidad, de forma que, en el primer nivel, proponía incluir en la normativa la obligación de cumplir con el requisito de los dos elementos esenciales del principio (adopción de medidas y asegurar la prueba de esa adopción). Este requisito sería obligatorio para todos los responsables aunque también añadía el GA29 que podía complementarse con otras obligaciones adicionales como realizar evaluaciones de impacto. En el segundo nivel el GA29 incluía aquellas medidas que los responsables pudieran decidir cumplir de forma voluntaria y que irían más allá de los requisitos mínimos derivados del mero cumplimiento de los principios de protección de datos, lo que quedaría fuera de la normativa. Dictamen 3/2010, sobre el principio de responsabilidad, *op. cit*., págs. 6 y 9.

reglamento obliga a los responsables no residentes en la UE, al nombramiento de un representante, cuyo papel, como veremos se amplía en el reglamento, respecto a la Directiva 95/46/CE. No se incluiría, sin embargo, en el reglamento la implicación de la dirección de la organización[1624]. No obstante, se compensa con la obligación del delegado de protección de datos de reportar a la dirección ejecutiva de la organización directamente (art. 36.2 PCE-RGPD).

Como ya hemos visto, el elemento esencial del principio de *accountability* consistente en la adopción de políticas y de medidas para aplicar estas políticas, se establece claramente en el reglamento (art. 22 PCE-RGPD) aunque hay que recordar las divergencias entre los enfoques de las instituciones. Ahora bien, respecto a las medidas en concreto que deben adoptarse, hay que decir que encontramos algunos ejemplos de medidas mencionadas en los instrumentos jurídicos examinados, en el reglamento. Esto se corresponde con el listado adoptado por la Comisión Europea que, ya en su propuesta, entendía que algunas de las obligaciones del responsable se integraban en este principio.

Así, en el reglamento se incluyen las obligaciones de conservación de documentación, incorporación de la *privacy by design* o *by default*, las evaluaciones de impacto o las notificaciones en caso de violación de datos. Otra medida que en los instrumentos jurídicos se incluía era la formación del personal implicado. No se ha incluido expresamente esta medida en el reglamento, aunque evidentemente es un aspecto que debe adoptarse[1625]. En este sentido, el GA29 afirmaba la importancia de la formación y consideraba que la aplicación de este principio podría contribuir al desarrollo de conocimientos jurídicos y técnicos, ya que precisaría de personas competentes en una multitud de aspectos con capacidades para comunicar, formar, establecer políticas,

[1624] A este respecto señalar por ejemplo la enmienda 2329 que proponía añadir un artículo 37 bis titulado "responsabilidad del consejo de la empresa" en el que el responsable y el encargado del tratamiento debían nombrar a un miembro del consejo de la empresa que fuera el responsable final de cumplir con las disposiciones del Reglamento. Enmiendas (7) 2091 – 2350, Proyecto de informe Jan Philipp Albrecht (PE501.927v04-00) sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) Propuesta de Reglamento, (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 6.3.2013.

[1625] Las enmiendas 1684 de Nils Torvalds y 1685 de Adina-Ioana Valean, Jens Rohde proponían incluir en el artículo 22.2 otra medida relativa a la existencia de una adecuada concienciación y formación del personal que participa en el tratamiento de datos y en las decisiones relativas al mismo. Enmiendas (5) 1493 – 1828, Proyecto de informe Jan Philipp Albrecht (PE501.927v04-00) sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) Propuesta de Reglamento, (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 6.3.2013.

realizar auditorías[1626]. De esta forma las autoridades de control dispondrían de interlocutores preparados que facilitarían la relación con los responsables.

Relacionada con la adopción de políticas y medidas estaba la necesaria adopción de sistemas de seguimiento y verificación del cumplimiento de las mismas. También hemos visto que, tanto la Comisión, como el Parlamento incluían mecanismos que incluían este aspecto en el desarrollo del principio.

El responsable debe ser capaz de demostrar que ha adoptado las medidas para cumplir la normativa. Esta característica se encuentra incorporada en el desarrollo del principio, como se ha visto. Asimismo, una de las obligaciones del responsable se referirá a la conservación de la documentación relativa a los tratamientos de datos que claramente apunta a esta necesidad de demostrar (art. 28 PCE-RGPD).

Además de que el responsable sea capaz de demostrar que ha adoptado todas estas medidas, surgía la pregunta de ¿ante quién debe demostrar el responsable que cumple con el principio? En el reglamento la respuesta serían las autoridades de control. Para reforzar este aspecto se ha recogido una obligación específica de cooperación del responsable y el encargado del tratamiento con la autoridad de control, de forma que deben facilitar la información que les pueda solicitar esta autoridad en el ejercicio de sus funciones (art. 29 PCE-RGPD). Esta obligación complementa y remite a la regulación de los poderes de investigación de las autoridades de control (art. 53.2 PCE-RGPD). El Consejo UE eliminó la obligación expresa de cooperación, pero hay que entender que subsiste la obligación implícita, al establecerse el poder de la autoridad de control a solicitar la información (art. 53.1 apartados a), a bis), d bis), d ter) PCJ-RGPD).

Por último, se señalaba la transparencia y los procedimientos para atender reclamaciones, como otros rasgos que caracterizan la *accountability*. Ambas características se incluyen en el reglamento, pese a que no se consideren medidas que deriven propiamente del principio de *accountability*.

[1626] Dictamen 3/2010, sobre el principio de responsabilidad, *op. cit*., pág. 18.

Así, la transparencia es uno de los pilares de la regulación, de forma que se incluye entre los principios relativos al tratamiento de datos personales[1627] y se desarrolla en la parte de los derechos de los interesados[1628]. Lo que se pretende con la transparencia es que los interesados estén informados de los tratamientos de datos personales que lleva a cabo el responsable y de establecer las vías para que puedan obtener esta información. No obstante, el Parlamento ha incluido, en el marco de la obligación de *accountability*, la necesidad de describir las medidas adoptadas en informes periódicos, que deba presentar el responsable (art. 22.3 PPE-RGPD).

Otra medida que proporciona transparencia es la designación del delegado de protección de datos, ya que se establece el derecho de los interesados a contactar con el mismo para poder plantearle cualquier cuestión relativa a la protección de datos (art. 35.10 PCE-RGPD).

En lo que se refiere a los procedimientos para atender reclamaciones, de la regulación del reglamento se extrae que el responsable deberá instaurar los procedimientos para tutelar los derechos que podrán ejercer los interesados (acceso, rectificación, supresión, oposición). Además, sin que se pueda considerar un mecanismo de *accountability*, hay que tener en cuenta que el reglamento dispone de recursos que podrán interponerse contra el responsable del tratamiento. No obstante, para cumplir enteramente con esta característica el responsable debería implantar procedimientos para poder atender cualquier otra reclamación del interesado e incluso, llegar a establecer mecanismos de indemnización sin necesidad de que el interesado deba acudir a las vías judiciales o administrativas[1629]. Esto podrá realizarse mediante la elaboración de los códigos de conducta, como se verá a continuación.

[1627] "Los datos personales deberán ser: a) tratados de manera lícita, leal y transparente en relación con el interesado;" (art. 5.a) PCE-RGPD). También consideraba el GA29 que la transparencia era un elemento integral en la *accountability*. Dictamen 3/2010, sobre el principio de responsabilidad, *op. cit*., pág. 15.

[1628] En el capítulo III del Reglamento, dedicado a los derechos del interesado, se encuentra la sección 1 relativa a la transparencia.

[1629] Entre las medidas que sugería el GA29 que podían derivarse del principio de *accountability* indicaba el establecimiento de un mecanismo interno de tratamiento de quejas y procedimientos internos de gestión y notificación de fallos de seguridad. Dictamen 3/2010, sobre el principio de responsabilidad, *op. cit*., pág. 13.

Hay que tener en cuenta que el incumplimiento del principio se establece como uno de los supuestos que genera la aplicación de una sanción[1630]. Para asegurar que se cumpliera con la *accountability*, el GA29 indicaba que era necesario que se establecieran sanciones en caso de incumplir este precepto y además que estas sanciones debían acumularse a las derivadas de la vulneración de los principios materiales de protección de datos[1631]. Esto derivaba del planteamiento del GA29, según el que cumplir con este principio no implicaba necesariamente que se cumpliera con los principios materiales[1632].

En lo que respecta a la actuación de las autoridades de control, el sistema de *accountability* implica que se dirija el control *a posteriori*, ya que se centrará en la supervisión de los resultados obtenidos por la actuación del responsable[1633]. Así, se pasa del esquema de la Directiva 95/46/CE que incluía la obligación de notificación de los tratamientos de datos a las autoridades de control y el control previo, a un control posterior que examine si el responsable ha conseguido el buen gobierno en materia de protección de datos[1634].

iii. Los códigos de conducta y la certificación

[1630] Así el artículo 79.6 PCE-RGPD indicaba que "la autoridad de control impondrá una multa de hasta 1.000.000 EUR o, si se trata de una empresa, de hasta el 2 % de su volumen de negocios anual a nivel mundial, a todo aquel que, de forma deliberada o por negligencia:" […] "e) no adopte políticas internas o no implemente medidas adecuadas para asegurar y demostrar la conformidad del tratamiento con los artículos 22, 23, y 30". El Parlamento no especificó las tipificaciones concretas. El Consejo estableció que "la autoridad de control podrá imponer una multa que no excederá de 1.000.000 EUR o, si se trata de una empresa, del 2% de su volumen de negocios mundial anual total del ejercicio económico anterior, al responsable o encargado del tratamiento que, de forma deliberada o por negligencia:" […] "d bis) no aplique las medidas adecuadas o no pueda demostrar la conformidad del tratamiento con los artículos 22 y 30" (art. 79bis.3.dbis PCJ-RGPD). Como indicaban DE HERT y STEFANATOU es cuestionable que se proporcione un auténtico incentivo al responsable para cumplir con el principio. El único incentivo (como indican gráficamente la "zanahoria") sería la mitigación de la sanción administrativa que sólo se contemplaba respecto a algunas de las medidas, como la de *privacy by design*. P. DE HERT, D. STEFANATOU, "The accountability culture in its european unión dress. Sticks but no carrots to make the proposed data protection regulation work", A. RALLO LOMBARTE, R. GARCÍA MAHAMUT (Ed.), VVAA, *Hacia un nuevo derecho europeo de protección de datos. Towards a new European data protection regime*, pág. 407.

[1631] Dictamen 3/2010, sobre el principio de responsabilidad, *op. cit*., pág. 18.

[1632] El GA29 señalaba que no podía establecerse una presunción jurídica de cumplimiento de estos principios materiales si se había cumplido con la *accountability*. Evidentemente, si se adoptaban las medidas adecuadas ello redundaría en una menor probabilidad de incumplir los principios materiales pero no por ello, automáticamente debía implicar que se eximiera al responsable. Sí admitía el GA29 que se podría tener en cuenta en el momento de evaluar la sanción. Dictamen 3/2010, sobre el principio de responsabilidad, *op. cit*., pag. 11.

[1633] Dictamen 3/2010, sobre el principio de responsabilidad, *op. cit*., pág. 18.

[1634] *Ibídem.*

Se mantiene en el reglamento una regulación que pretende, al igual que sucede en la Directiva 95/46/CE, la promoción de los códigos de conducta. Para ello, se otorga la posibilidad de que asociaciones y organismos que representen a categorías de responsables o encargados del tratamiento y que elaboren, modifiquen o amplíen códigos de conducta, puedan presentarlos ante la autoridad de control o ante la Comisión (si la entidad tiene un alcance de más de un Estado miembro), con el fin de que emitan un dictamen acerca de la conformidad con el reglamento (art. 38 apdos. 2 y 3 PCE-RGPD)[1635]. El Parlamento estableció que, además de las asociaciones, las autoridades de control también pudieran elaborarlos (art. 38.1 PPE-RGPD).

El Consejo UE ha incidido en la supervisión del cumplimiento del código, de forma que, sin perjuicio de las funciones de las autoridades de control, ha establecido que el código de conducta debe incluir mecanismos que permitan su supervisión por un organismo específico que será acreditado por la autoridad de control competente (art. 38.1ter y 38bis.1 PCJ-RGPD). Este organismo, que se regula en el texto del Consejo UE, podrá adoptar medidas en caso de infracción del código por un responsable o encargado, incluyendo la suspensión o exclusión (art. 38bis.4 PCJ-RGPD). El organismo informará a la autoridad de control sobre la adopción de estas medidas.

No obstante, un aspecto que no se encontraba en la Directiva 95/46/CE son los mecanismos de certificación. Y es que el principio de *accountability* enlaza con el desarrollo de sistemas de certificación, de forma que parece una evolución natural. En un primer momento, el responsable del tratamiento debe instaurar las medidas adecuadas para cumplir con la normativa. Posteriormente, el responsable del tratamiento podría acudir a un sistema de certificación que evaluase que efectivamente aplica estas medidas. De esta forma, el responsable podría obtener un certificado o sello que hiciera visible su esfuerzo en asegurar un correcto cumplimiento[1636]. Por tanto, el responsable obtendría así

[1635] Respecto a esta segunda posibilidad de presentar el código a la Comisión, hay que indicar que el Consejo UE ha modificado el trámite. Cuando el código afecte a actividades de tratamiento en varios Estados miembros de la UE, la asociación podrá presentarlo a la autoridad de control competente y ésta emitirá un dictamen sobre si el código es conforme con el Reglamento. Antes de su aprobación, se dirigirá al Consejo Europeo de Protección de Datos (que sustituirá al GA29), que dictaminará si cumple con el Reglamento. Si el dictamen confirma que cumple la normativa el Consejo Europeo de Protección de Datos someterá su dictamen a la Comisión, que podrá adoptar un acto de ejecución para aprobar que el código tenga validez dentro de la UE. (art. 38 apdos. 2 a 4 PCJ-RGPD).

[1636] La Propuesta de Madrid también incluye entre las medidas proactivas establecidas: "la adhesión a acuerdos de autorregulación cuya observancia resulte vinculante, que contengan elementos que permitan

una forma de diferenciarse en el mercado. Además, este sistema de certificación se puede utilizar para facilitar la supervisión que las autoridades de protección de datos puedan llevar a cabo.

Hay que recordar las iniciativas existentes en materia de certificación y de normalización que se comentaban al abordar la obligación de seguridad en el marco de la Directiva 95/46/CE, tanto a nivel de la UE como de las legislaciones nacionales[1637]. Tanto los códigos de conducta como los mecanismos de certificación incluidos en el reglamento constituyen el resultado de la tendencia que se señalaba en la utilización de fórmulas de autorregulación regulada. Esto implica la autorregulación por parte de los responsables

---

medir sus niveles de eficacia en cuanto al cumplimiento y grado de protección de los datos de carácter personal, y establezcan medidas efectivas en caso de incumplimiento."(22.g Propuesta de Madrid). También se desarrolló un proceso de autorregulación que llevaba al otorgamiento de un sello en el marco del APEC Privacy Framework. Este instrumento instaba al desarrollo de un sistema de reglas no vinculantes para la protección de la privacidad, en las transferencias internacionales de datos. En consecuencia, se elaboró el denominado *APEC Data privacy pathfinder,* en septiembre de 2007, y que consistía en un proyecto de cooperación entre los Estados miembros para desarrollar el sistema al que podrían acogerse las organizaciones interesadas. El sistema desarrollado que se denomina *APEC Cross-Border Privacy Rules* (CBPR) se conforma de una serie de mecanismos: un cuestionario de autoevaluación para la organización solicitante sobre los principios de privacidad, *CBPR Intake questionnaire, 2011/SOM1/ECSG/DPS/020*; un documento que contiene los requisitos básicos que se fundamentan en los nueve principios de privacidad y que le servirán a un Agente de *Accountability*, reconocido por la APEC, para evaluar un cuestionario de autoevaluación, cumplimentado por una organización, *CBPR Program Requirements for use by Accountability Agents*; los criterios de reconocimiento que utilizarán los Estados miembros de la APEC para reconocer a un Agente de Accountability, *Accountability Agent Recognition Criteria, 2010/SOM1/ECSG/DPS/011*; el acuerdo de aplicación de la privacidad transfronteriza, *the Cross Border Privacy Enforcement Cooperation Agreement, 2010/SOM1/ECSG/DPS/013* y la Carta de reglas de privacidad transfronteriza del panel conjunto de revisión, *Charter of the Cross Border Privacy Rules Joint Oversight Panel. Guidebook on APEC privacy and trustmark, APEC#212-CT-03.2, Electronic Commerce Steering Group*, APEC, Noviembre 2012, págs. 26 a 28, http://publications.apec.org/publication-detail.php?pub_id=1345 (fecha consulta: 11.8.2014). Así las organizaciones del sector privado que estén interesadas pueden acogerse a este sistema CBPR y obtener la certificación de que cumplen sus requisitos. Para ello, deben adoptar políticas y prácticas que protejan la privacidad, de acuerdo con lo establecido en el sistema CBPR. Estas políticas y prácticas son evaluadas por un Agente de *Accountability*, reconocido previamente por la APEC, que revisa que cumplen con el sistema CBPR. Una vez se certifica a la organización solicitante, sus políticas y prácticas son vinculantes y la revisión de su cumplimiento por parte de la organización, podrá realizarse por la autoridad de protección de la privacidad. Para ello se ha creado un marco de colaboración entre las diferentes autoridades mediante el CPEA mencionado. Mientras se discute la validez de la decisión de *Safe Harbour*, la UE, a través del GA29, y la APEC, a través del Subgrupo de privacidad de datos, han trabajado en un documento de referencia para facilitar a las organizaciones la tramitación de las BCR europeas y del CBPR de la APEC. En el documento se deja claro que no se trata de un reconocimiento mutuo de los sistemas, sino que el objetivo es proporcionar a las organizaciones una comparativa entre ambos sistemas, de forma que muestra los puntos en común y, lo más importante, las diferencias que deben ser tenidas en cuenta, a la hora de someterse a ambos sistemas. De esta forma, las organizaciones, a la hora de decidir las políticas internas que pretenden adoptar, lo harán teniendo en cuenta estos elementos, con vistas a poder obtener el visto bueno en ambos sistemas. Dictamen 02/2014 sobre un documento de referencia para los requisitos en materia de normas corporativas vinculantes presentadas a las autoridades nacionales de protección de datos en la UE y normas de privacidad transfronterizas remitidas a los agentes de rendición de cuentas de dichas normas de la APEC, 538/14/ES, WP 212, 27.2.2014, Grupo de trabajo Artículo 29 sobre la protección de datos.

[1637] Ver Capítulo V.

aunque sometida a una regulación y a una supervisión por parte de las autoridades de control o los organismos acreditados con este fin[1638].

El desarrollo de estos mecanismos de certificación ha adquirido progresivamente relevancia durante el proceso legislativo. En el texto inicial se establecía básicamente una invitación a los Estados miembros y a la Comisión para promoverlos y se facultaba a esta última a adoptar criterios, requisitos o mecanismos y normas técnicas relacionados con la certificación (art. 39 PCE-RGPD). Se establecía la posibilidad de sancionar con una multa de hasta 1.000.000 € o el 2% del volumen del negocios anual a nivel mundial, a todo aquel que hiciera uso indebido de estos sellos o marcas (art. 79.6.k) PCE-RGPD).

El Parlamento concretó la regulación y estableció la posibilidad de que los responsables o los encargados pudieran solicitar a cualquier autoridad de control de la UE que certificara que el tratamiento de datos lo efectuaban de conformidad con el reglamento (art. 39.1bis PPE-RGPD). Para ello, disponía que las autoridades pudieran acreditar a auditores que serían los que llevarían a cabo la auditoría, aunque la certificación la otorgaría la autoridad de control (art. 39.1quinquies PPE-RGPD). Esta certificación consistiría en la concesión de la marca denominada "Sello Europeo de Protección de Datos", que sería válida durante un máximo de cinco años (art. 39.1sexies PPE-RGPD). Además, se incluía la posibilidad de que el Consejo Europeo de Protección de Datos pudiera certificar la conformidad con el reglamento de normas técnicas (art. 39.1decies PPE-RGPD).

El Consejo UE ha dado un paso más y ha establecido que la certificación la puedan otorgar, además de las autoridades de control, los organismos de certificación (art. 39.2bis PCJ-RGPD). Estos organismos deberán evaluar el cumplimiento del reglamento por parte de los responsables y los encargados del tratamiento y comunicarán a la autoridad de control motivadamente, tanto el otorgamiento, como la retirada de la certificación (art. 39bis.4 y .5 PCJ-RGPD). El Consejo UE no ha concretado, como el Parlamento ningún sello específico, sino que ha desarrollado una regulación sobre los

[1638] TRONCOSO REIGADA estima que sería razonable una cierta implicación de las autoridades de control en el modelo de certificación, aunque advierte que no deben confundirse los reguladores (las autoridades de control) con los regulados (que serían las autoridades de certificación y las empresas de auditoría). A. TRONCOSO REIGADA, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *Revista Española de Derecho Europeo, op. cit.*, págs. 22

requisitos que deben cumplir estos organismos de certificación. Los Estados miembros decidirán si pueden acreditar a estos organismos las autoridades de control o el Organismo Nacional de Acreditación (art. 39bis.1 PCJ-RGPD).

El Consejo UE ha sido el que ha impulsado decididamente, en su orientación general, la autorregulación. Ya vimos que había previsto que la adhesión a códigos de conducta o los mecanismos de certificación podían ser utilizados como elementos para demostrar el cumplimiento de las obligaciones del responsable (art. 22.2ter PCJ-RGPD). Pero lo más importante es que el Consejo UE, si bien, al igual que la Comisión también ha previsto una sanción por el uso indebido de los sellos o marcas (art. 79bis.3.f) PCJ-RGPD), por otro lado, ha establecido que la utilización de estos instrumentos sea un factor que ayude a reducir las sanciones administrativas que puedan imponerse a responsable o encargado, si se han adherido a algún código o a algún mecanismo de certificación (art. 79.2bis j) PCJ-RGPD). Es esencial que se otorgue algún incentivo cuando se usen estos instrumentos, ya que supone una inversión en tiempo y recursos por parte de los responsables[1639].

Otro aspecto novedoso incluido por el Consejo UE es la posibilidad de que responsables o encargados no sujetos al reglamento, puedan adherirse a los códigos de conducta o a los mecanismos de certificación, con el fin de que sirvan como garantías para poder realizar transferencias internacionales de datos (arts. 38.1bis y 39.1bis PCJ-RGPD).

2.2.2. Obligaciones derivadas del estatuto

a. Evaluación de impacto

La evaluación de impacto ya se realiza actualmente, como el proceso previo al tratamiento, en el que se analiza en clave de riesgos cómo afecta un determinado tratamiento en el derecho a la protección de datos y las medidas que deben adoptarse para

[1639] Como se mencionaba anteriormente, se trata de que se vea claro cual es la "zanahoria". P. DE HERT, D. STEFANATOU, "The accountability culture in its european unión dress. Sticks but no carrots to make the proposed data protection regulation work", A. RALLO LOMBARTE, R. GARCÍA MAHAMUT (Ed.), VVAA, *Hacia un nuevo derecho europeo de protección de datos. Towards a new European data protection regime*, pág. 407.

cumplir con la normativa. No obstante, la evaluación de impacto es más conocida por su denominación inglesa: *Privacy Impact Assessment* o PIA. Algunas autoridades de control han publicado guías para realizar esta evaluación, entre las que se cuentan la AEPD que elaboró la guía tras un proceso de consulta pública[1640].

La evaluación de impacto se conecta con el trámite de consulta previa a la autoridad de control, de forma que, según el resultado que el responsable o el encargado obtengan deberán consultar o no a la autoridad. De esta forma, la Comisión, explicaba en su propuesta, que con esta medida, se contrarrestaba la eliminación de la obligación de notificación general de los tratamientos a la autoridad de control (Considerando 70 PCE-RGPD). Su regulación ha sufrido algunos cambios en el devenir legislativo, especialmente en el trámite parlamentario.

En el texto inicial de la Comisión, la evaluación de impacto debía realizarla el responsable o el encargado, cuando la operación de tratamiento entrañara riesgos específicos para los derechos y libertades de los interesados en razón de su naturaleza, alcance o fines (art. 33.1 PCE-RGPD). Por tanto, se formaliza la necesidad de llevar a cabo un proceso de reflexión y análisis previo a la realización del tratamiento. Este proceso refleja la necesaria ponderación que debe llevar a cabo el responsable (y también el encargado) antes de iniciar el tratamiento. No es que aparezca tal necesidad de realizar esta ponderación con el reglamento, sino que se hace visible y se configura como obligatoria. También hay que alertar sobre la referencia a "derechos y libertades", por lo que no sólo deberá tenerse en cuenta en este análisis el derecho de protección de datos.

Con el fin de dar unas pautas de lo que se debían considerar "operaciones de tratamiento que entrañen riesgos específicos", se incluyeron algunas a modo ejemplificativo (art. 33.2 PCE-RGPD). Las operaciones que se establecen responden a tratamientos como los dedicados a evaluar aspectos personales, con el fin de adoptar medidas, o tratamientos a gran escala de categorías especiales de datos, o tratamientos

[1640] Guía para una Evaluación de Impacto en la protección de datos personales, publicada el 29 de octubre de 2014. Agencia Española de Protección de Datos. http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf, (fecha consulta: 27.12.2014). También baste citar la guía de la autoridad de control inglesa: *Conducting privacy impact assessments code of practice, Information Commissioner's Office* (ICO), 25.2.2014. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf, (fecha consulta: 27.12.2014).

que respondan al seguimiento de zonas de acceso público. Asimismo, se incluye una vía para ampliar el listado de supuestos, ya que se incluirán aquellos tratamientos que la autoridad de control considere que precisan de consulta previa por entender que probablemente entrañen riesgos específicos para los derechos y libertades de los interesados (arts. 33.2.e) y 34.2.b) PCE-RGPD).

Se estableció un contenido mínimo que debía incluir la evaluación y la obligación del responsable de recabar la opinión de los interesados (art. 33.3 y .4 PCE-RGPD). Asimismo, se eximió de llevar a cabo la evaluación a las autoridades u organismos públicos cuando llevaran a cabo el tratamiento para cumplir con una obligación legal (art. 33.5 PCE-RGPD)

En el trámite parlamentario, se modificó la rúbrica de la Sección, donde se encuentra esta obligación y la de autorización y consultas previas, de forma que, en vez de “Evaluación de impacto relativa a la protección de datos y autorización previa”, se tituló: “Gestión de la protección de datos durante el ciclo de vida”. Como ya he indicado, pese a que he incluido esta obligación en la fase previa, se aprecia el carácter de transversalidad prácticamente en todas las obligaciones. No obstante, sería también lógico que se incluyeran en esta gestión ambientada en el ciclo de vida del tratamiento de datos otras medidas, como las de protección de datos desde el diseño y protección de datos por defecto, que claramente deben situarse en el momento previo a realizar el tratamiento, es decir en la fase de desarrollo de los sistemas de tratamiento y, sin embargo, no se han incluido.

Este cambio dirigido a reflejar la transversalidad de la evaluación responde a la inclusión, en esta Sección, de otra obligación, consistente en una revisión del cumplimiento que deberá realizarse dos años después de llevar a cabo la evaluación de impacto y, a partir de ese momento, periódicamente, cada dos años o cuando hubiera un cambio en los riesgos de las operaciones de tratamiento (art. 33bis PPE-RGPD). Se ha huido de la calificación de esta obligación como una auditoría, sin duda, para relajar la exigencia que implicaría la auditoría respecto al deber de independencia por parte del auditor. De esta forma, se configura como una revisión a nivel interno, aunque se obliga a que si hay designado un delegado de protección de datos, se le implique en la revisión (art. 33 bis.5 PRGPD).

A esa obligación posterior a la evaluación de impacto, el Parlamento añadió otra previa: el análisis de riesgos (art. 32bis PPE-RGPD) que se incluye en la Sección, dedicada a la seguridad, por lo que se tratará en ese apartado. No obstante, hay que tener en cuenta que, solo en los casos previstos en que se considera que concurren riesgos específicos y que se incluyen en el precepto, dedicado a este análisis de riesgos, es cuando se tendrá que llevar a cabo la evaluación de impacto. Se amplían los supuestos respecto al texto de la Comisión y, por ejemplo, se incluyen tratamientos que afecten a más de cinco mil interesados durante doce meses o los que son susceptibles de sufrir una brecha de seguridad. Asimismo, se elimina la exclusión relativa a las entidades del sector público que había introducido la Comisión.

El Consejo UE estableció la necesidad de proceder a la evaluación de impacto cuando el tratamiento supusiera un alto riesgo para los derechos y libertades de las personas. El Consejo UE, por tanto, ha reducido especialmente el alcance de la obligación al establecer este alto riesgo, en vez de riesgo específico, como se describía en los textos anteriores. Este alto riesgo existirá cuando hayan "problemas de discriminación, usurpación de identidad o fraude, pérdidas económicas, menoscabo de reputación, cambio no autorizado de la seudonimización, pérdida de confidencialidad de datos sujetos al secreto profesional o cualquier otro perjuicio económico o social significativo" (art. 33.1 PCJ-RGPD).

Se incluyen algunos supuestos que se considera que supondrán este alto riesgo que, son la elaboración de perfiles, que impliquen adopción de decisiones con efectos jurídicos, el tratamiento de categorías especiales de datos y el seguimiento a gran escala de zonas de acceso público. No obstante, de nuevo se deja la posibilidad de que la autoridad de control especifique otros supuestos que exijan la realización de la evaluación (art. 33.2bis PCJ-RGPD), pero también que especifique supuestos en los que no es necesaria la evaluación (art. 33.2ter PCJ-RGPD). Otra novedad introducida por el Consejo UE es la alusión a los códigos de conducta para tenerlos en cuenta en el análisis del impacto de las operaciones de tratamiento, lo que resulta algo confuso (art. 33.3bis PCJ-RGPD).

La regulación de la evaluación de impacto ha tenido en cuenta los supuestos de

tratamiento que se han considerado que tienen más riesgos para los derechos, como son los que suponen un tratamiento masivo de datos o los que tienen como objetivo evaluar o predecir la conducta mediante la aplicación de perfiles. No obstante, esta obligación supondrá una ardua labor de concienciación de los responsables, que deben ser quienes determinen el nivel de riesgo que atribuyen al tratamiento y, más relevante, deben decidir si consultan a la autoridad, con todos los inconvenientes que esto puede suponer. También exigirá que las autoridades de control puedan asumir el impacto de tener que asesorar a los responsables.

b. Autorización y consultas previas

Como se ha indicado, la obligación de notificación a la autoridad de control que establece la Directiva 95/46/CE (arts. 18 ss.) desaparece del reglamento. En su lugar, la Comisión incluyó un supuesto en el que sería necesario solicitar autorización de la autoridad de control antes de tratar datos en caso de transferencias de datos a territorios u organizaciones internacionales que no cuenten con el nivel adecuado de protección (art. 34.1 PCE-RGPD), supuesto que se eliminó en los textos del Parlamento y del Consejo UE, por repetir lo que ya se indicaba en la parte relativa a las transferencias internacionales. Asimismo, se incorporó la obligación del responsable o del encargado, de consultar a la autoridad de control, antes de realizar el tratamiento, en dos casos: cuando la evaluación de impacto indique que hay un elevado riesgo o cuando la autoridad haya establecido que es necesaria la consulta (art 34.2 PCE-RGPD). La autoridad, si considera que el tratamiento no cumple con el reglamento, lo prohibirá y propondrá medidas para remediarlo (art 34.3 PCE-RGPD).

Los Estados miembros también deben consultar a la autoridad de control cuando elaboren una medida legislativa que defina la naturaleza del tratamiento, para garantizar su conformidad con el reglamento (art. 34.7 PCE-RGPD).

El Parlamento modificó esta disposición, de forma que si se hubiera designado delegado de protección de datos, la consulta se realizaría a este (art 34.2 PPE-RGPD)[1641].

[1641] Por tanto, sólo si no hay designado delegado deberá realizarse el trámite de consulta a la autoridad. Sin embargo en caso de que se consulte a la autoridad, ésta podrá llegar a prohibir el tratamiento si considera que el mismo no es conforme con el reglamento. Este aspecto puede hacer pensar que los responsables

Asimismo, en vez de ser la autoridad la que establece los supuestos en los que será necesaria la consulta, será el Consejo Europeo de Protección de Datos.

El Consejo UE sólo exige la consulta previa a la autoridad de control, en el caso de que la evaluación de impacto indique que el tratamiento entrañe un nivel de riesgo elevado (art 34.2 PCJ-RGPD). Además, si la autoridad considera que el tratamiento no está conforme, lo que hace el texto es establecer un proceso de asesoramiento por parte de la autoridad al responsable que deberá durar como máximo seis semanas prorrogables a otras seis, pero no indica nada respecto a las consecuencias de que se acabe este plazo y se mantenga el incumplimiento (art 34.3 PCJ-RGPD).

El Consejo UE mantiene la consulta en el supuesto de medidas legislativas (art 34.7 PCJ-RGPD). Asimismo, permite que los Estados miembros exijan a los responsables que realicen la consulta y obtengan autorización respecto a tratamientos en ejercicio de un interés público, como la protección social o la salud pública (art 34.7bis PCJ-RGPD).

c. *Privacy by design* y *Privacy by default*

En el reglamento se incorporan estos dos principios, protección de datos desde el diseño (*privacy by design*) y protección de datos por defecto (*privacy by default*) que, como ya vimos, pretenden incorporar la protección de datos, desde el primer momento, en el desarrollo de sistemas y aplicaciones informáticas[1642]. No obstante, de acuerdo con la transversalidad apuntada de los preceptos, se ha extendido la aplicación de estos principios a todo el ciclo de vida del tratamiento. De esta forma, se pretende que las herramientas tecnológicas utilizadas para llevar a cabo el tratamiento de datos permitan cumplir con el reglamento.

i. Privacy by design

La Comisión, en su propuesta, definía la *privacy by design*, como la obligación del responsable de implementar, tanto en el momento de determinación de los medios como

podrán preferir designar un delegado antes que tener que dirigir las consultas a la autoridad de control. Será, por tanto, primordial el papel que juegue el delegado de protección de datos en la supervisión del tratamiento.

[1642] Ver Capítulo V.

durante el tratamiento, en virtud de las técnicas existentes y los costes, las medidas y procedimientos técnicos y organizativos apropiados, de forma que el tratamiento sea conforme al reglamento y garantice la protección de los derechos de los interesados (art. 23 PCE-RGPD). Por tanto, se trata de medidas técnicas que se caracterizan especialmente por tener que implantarse desde el momento de determinación de los medios, es decir, desde la fase de desarrollo y que serán instrumentos para cumplir con el reglamento.

En el procedimiento legislativo se ha modificado esta disposición. En el Parlamento se incluyeron más factores a tener en cuenta a la hora de adoptar las medidas, aunque se eliminaron los costes: técnicas existentes, conocimientos técnicos, mejores prácticas y riesgos (art. 23.1 PPE-RGPD). Si bien se mantuvo la esencia del principio, se especificó que las medidas debían adoptarse en el momento de determinación de los fines y los medios, así como durante el tratamiento. Las medidas debían asegurar el cumplimiento con el reglamento pero se especificaba que, en particular, con los principios de protección de datos incluidos en el artículo 5. Asimismo, se enfatizó que la obligación debía extenderse a la gestión del ciclo de vida del tratamiento, que se tendría en cuenta la evaluación de impacto en la adopción de medidas y, con el fin de incentivar su uso, se estableció como requisito previo para licitaciones en contratos públicos (art. 23bis PPE-RGPD).

Otro aspecto relevante que introdujo el Parlamento es que serían sujetos obligados el responsable y el encargado. Hay que entender que pese a que la obligación se sitúe en el momento de la determinación de los fines y los medios, no impide que sea el encargado quien tenga que cumplirlo.

El Consejo UE modificó el precepto, de manera que no incluyó la referencia al momento de aplicación del principio e incrementó los factores a tener en cuenta a la hora de la adopción de las medidas: técnicas existentes, coste, naturaleza, ámbito, contexto y fines del tratamiento, probabilidad y gravedad del riesgo para los derechos (art. 23.1 PCJ-RGPD). Las medidas deben asegurar el cumplimiento del reglamento y se señalan, como ejemplos, la minimización y el uso de seudónimos[1643].

[1643] El Consejo UE añadió más ejemplos de medidas en la parte de los Considerandos: transparencia respecto a las funciones y al tratamiento, permitir a los interesados supervisar el tratamiento, permitir al responsable crear y mejorar la seguridad. Asimismo se incluyó una referencia al necesidad de animar a los

El texto del Consejo UE mantuvo la obligación para el responsable e incluyó la posibilidad de acudir a mecanismos de certificación para demostrar la conformidad de las medidas, tanto en este caso, como en el de *privacy by default* (art. 23.2bis PCJ-RGPD).

ii. Privacy by default

La Comisión definió la *privacy by default* como la utilización de mecanismos que garanticen que, por defecto, sólo sean objeto del tratamiento los datos personales necesarios para cada fin específico del tratamiento y que no se recojan ni conserven más allá del mínimo necesario (art. 23.2 PCE-RGPD). Estos mecanismos permitirán que los datos no sean accesibles a un número indeterminado de personas. El Parlamento sólo añadió que también deberían permitir al interesado controlar la divulgación de sus datos (art. 23.2 PPE-RGPD). El Consejo UE modificó este último aspecto, de forma que sólo se aplicara cuando el fin del tratamiento no fuera facilitar información al público y, en este caso, los mecanismos habilitados debían garantizar que los datos no fueran accesibles sin intervención humana a un número indeterminado de personas (art. 23.2 PCJ-RGPD).

La *privacy by default* lo que hace, al igual que la *privacy by design* es adoptar un enfoque práctico, de manera que incentiva que se tengan en cuenta los principios de protección de datos en un momento relevante, como es el de diseño de las herramientas que se utilizarán para el tratamiento. Por tanto, son obligaciones que se añadirían a las materiales, propias de la regulación y que son características de la *accountability*. Así, la *privacy by default* aplica esencialmente el principio de calidad o minimización de los datos.

d. Conservación de documentación

Esta obligación responde plenamente al principio de *accountability*, de forma que su objetivo es que el responsable pueda demostrar que cumple con lo establecido en el reglamento frente a las autoridades de control. Por tanto, estamos ante una obligación

fabricantes y desarrolladores para que tuvieran en cuenta la protección de datos en el desarrollo y diseño de sus productos y servicios para asegura que responsables y encargados estuvieran en disposición de cumplir con sus obligaciones (Considerando 61 PCJ-RGPD).

formal y que implica la puesta a disposición, de esta documentación, a la autoridad de control (art. 28.3 PCE-RGPD)[1644].

Durante el proceso legislativo se redujo el alcance de la obligación. De esta forma, inicialmente la Comisión había previsto la obligación de conservar la documentación de todas las operaciones del tratamiento y había incluido un mínimo de información que debía contener la documentación. Se trataba de un listado bastante amplio descriptivo de las operaciones y de todos los sujetos implicados. Asimismo, en este texto inicial, se establecieron como sujetos obligados a cumplirla, no sólo el responsable, sino también el encargado y el representante del responsable.

El Parlamento y el Consejo UE redujeron el mínimo de información que debía conservarse. El primero prefirió incluir una obligación más general de conservación de la documentación necesaria para cumplir con el reglamento (art. 28.1 PPE-RGPD). El Consejo UE lo que hizo fue configurar la obligación como la llevanza de un registro, en el que la información contenida fuera referida a categorías, de forma que no se concretara. Por ejemplo, se debía conservar la información de categorías de destinatarios, no de destinatarios concretos. Respecto a ciertos aspectos problemáticos, como los plazos de conservación de los datos, se indicaba que debían incluirse en el registro, cuando fuera posible (art. 28.1 PCJ-RGPD). Otra novedad que incluyó el Consejo UE fue diferenciar la información mínima que debían registrar el responsable o su representante y la que debía conservar el encargado (art. 28.2bis PCJ-RGPD).

En la propuesta inicial de la Comisión se preveía una excepción en la aplicación de esta obligación para las personas físicas que trataran datos sin interés comercial y para empresas u organizaciones que emplearan a menos de 250 personas y que trataran datos personales sólo como actividad accesoria a sus actividades principales (art. 28.4 PCE-RGPD). Esta excepción fue suprimida por el Parlamento. El Consejo UE eliminó la excepción para las personas físicas y dejó la referida a las empresas, aunque especificó que no regiría si el tratamiento diera lugar a un riesgo alto para los derechos y libertades de los interesados (art. 28.4.b) PCJ-RGPD).

[1644] No obstante, el Parlamento eliminó esta especificación relativa a la puesta a disposición, por lo que primó el objetivo de control interno del responsable, al de control externo por parte de la autoridad.

e. Seguridad

La obligación de seguridad ha sufrido cambios sobre todo durante el proceso parlamentario, especialmente relacionados con otras obligaciones, como ya se adelantó: la evaluación de impacto y el análisis de riesgos.

La Comisión, inicialmente había previsto, por un lado, la obligación de seguridad que tenían responsable o encargado del tratamiento, consistente en adoptar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado con relación a los riesgos que entrañara el tratamiento y la naturaleza de los datos (art. 30.1 PCE-RGPD). Se exigía que para adoptar estas medidas el responsable o el encargado debían llevar a cabo una evaluación de riesgos.

Por otro lado, se establecía la obligación del responsable o el encargado de llevar a cabo una evaluación de impacto, cuando las operaciones de tratamiento entrañasen riesgos específicos para los derechos y libertades de los interesados (art. 33.1 PCE-RGPD). Además, se enumeraban algunas operaciones que ya se consideraba que entrañaban estos riesgos específicos (art. 33.2 PCE-RGPD).

En el trámite parlamentario se modificaron estas obligaciones, de manera que la obligación relativa a la seguridad exige la adopción de las medidas, tal como establecía la propuesta de la Comisión, para garantizar el nivel de seguridad con relación a los riesgos del tratamiento pero se añade que se tomará en consideración la evaluación de impacto (art. 30.1 PPE-RGPD). Por tanto, se conectan la obligación de seguridad con la evaluación de impacto. Además, se incluye, a diferencia del anterior texto, el desarrollo de una medida a adoptar que es la política de seguridad, de la que se especifica su contenido (art. 30.1bis PPERGPD)[1645]. También se incorporan los objetivos que deben perseguir estas medidas de seguridad (art. 30.2 PPE-RGPD)[1646].

[1645] Entre los cambios que se han producido en el trámite parlamentario, no me parece acertada la introducción de este artículo 30.1bis PPE-RGPD que constituye un concreción innecesaria respecto a algunos aspectos que debe incluir la política de seguridad. Lo más adecuado sería remitirse a los estándares existentes en materia de seguridad de la información que reflejan las metodologías que se adoptan actualmente y que han alcanzado una madurez que estas disposiciones no pueden igualar.

[1646] Tampoco me parece acertada la modificación del apartado 2 de este artículo 30 PPE-RGPD, con el fin de ajustarlo a la formulación que se realiza en la Directiva sobre privacidad y comunicaciones electrónicas para evitar dos conjuntos distintos de normas para una única empresa, tal como se señala en la enmienda que introduce el cambio, enmienda 1928, 2, Enmiendas (6),1829 – 2090, Proyecto de informe Jan Philipp

Si bien se elimina del precepto la referencia a la evaluación de riesgos, lejos de abandonar el texto parlamentario esta metodología, lo que hace es regular en un nuevo artículo la necesidad de llevar a cabo un análisis de riesgos (art. 32bis PPE-RGPD). Este análisis de riesgos se establece como un paso previo a la evaluación de impacto ya que su objetivo es detectar si es probable que las operaciones de tratamiento presenten riesgos específicos (art. 32bis.1 PPE-RGPD). Se incluyen también, al igual que sucedía en el texto anterior respecto a la evaluación de impacto, algunas operaciones que se considera que es probable que presenten estos riesgos específicos (art. 32bis.2 PPE-RGPD). Por tanto, en este caso, a diferencia del texto de la Comisión, se considera que es probable que entrañen estos riesgos, no que seguro que los entrañen.

Pues bien, respecto a estos supuestos que se enumeran como susceptibles de entrañar riesgos específicos, se establecen diversas acciones a adoptar dirigidas a reforzar la protección de los tratamientos. Entre estas acciones se encuentra la evaluación de impacto (art. 32bis.3.c PPE-RGPD). Por tanto, la evaluación de impacto sólo deberá realizarse, según el texto parlamentario, en los supuestos enumerados, es decir, respecto a todos los que indica el precepto excepto uno (art. 33.1 PPE-RGPD)[1647].

En referencia al enfoque adoptado de riesgos, el GA29 alertó sobre la visión errónea que parecía extenderse sobre esta metodología relativa a que podía ser una alternativa a los derechos y principios de protección de datos, en vez de una manera de adaptar el cumplimiento de forma que fuera escalable[1648]. Por eso, el GA29 publicó un manifiesto en el que recordó que el derecho a la protección de datos es un derecho

Albrecht (PE501.927v04-00) sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) Propuesta de Reglamento, (COM(2012)0011–C7-0025/2012 – 2012/0011(COD)), 6.3.2013.

[1647] Así, aunque la lista de casos que entrañan riesgos se plantee como no exhaustiva, lo cierto es que la evaluación de impacto sólo debe efectuarse en estos casos, aunque se establece la vía para ampliar estos supuestos que requerirán de evaluación si el delegado de protección de datos o la autoridad de control estiman que hay operaciones de tratamiento que pueden suponer riesgos específicos y, por tanto, exigen de consulta previa (arts. 32bis.2.f PPE-RGPD). En caso de considerar que hay riesgos específicos, si no se puede encajar el supuesto en la lista, no habría aparentemente ninguna consecuencia. No se señala ninguna consecuencia para uno de los supuestos señalados en la lista, en concreto el apartado i) del artículo 32bis.2 PPE-RGPD. Si bien es cierto que este supuesto hace referencia a "la facilitación de datos personales a un gran número de personas que no cabe esperar razonablemente que sea limitado", por lo que alude, por ejemplo, a la publicación de datos en Internet que podrían llevar a cabo los particulares. Se entiende que, en este caso, lo que se pretende es no obligar a estos particulares a realizar la evaluación de impacto.

[1648] *Statement on the role of a risk-based approach in data protection legal frameworks, op. cit.*, pág. 2.

fundamental y cualquier operación de tratamiento debía respetarlo[1649]. Los derechos que la ley brinda a los titulares de datos personales debían ser respetados, independientemente del nivel de riesgo que pudiera afectar al tratamiento de datos[1650].

Al debate parlamentario se añadió también el debate público que se había originado entorno al *big data.* Autores estadounidenses apuntaban a que debería hacerse más hincapié en el uso de los datos que en la recogida[1651]. Así, se pretendía partir de la idea de que en Internet no se puede evitar que se vuelque información y tampoco sería positivo, ya que no se podría sacar el máximo partido a esta herramienta. Por tanto, la protección de los datos no debía consistir en evitar que circularan, sino que lo importante sería limitar los usos que los sujetos pudieran hacer de los mismos[1652]. Así se pretendía fomentar un sistema basado en los daños con un control *a posteriori* y un enfoque orientado a la gestión de riesgos, que dejara en manos del responsable la protección.

Sin embargo, el GA29 respondió a estas propuestas, en una declaración sobre el *big data*[1653]. El GA29 indicó que no sólo debía incidirse en el uso de los datos, sino que los principios de limitación de fines y de minimización de datos debían ser aplicados.

[1649] *Ibídem*, pág. 3.

[1650] Dejó claro el GA29 que el nivel de riesgo podía determinar el grado de cumplimiento de algunas obligaciones derivadas de la *accountability*, de forma que algunas podrían, incluso no aplicarse, pero no podía determinar el grado de cumplimiento de las obligaciones de protección de datos. Los principios aplicables a los responsables (legitimación, minimización, limitación de fines, transparencia, integridad de los datos, exactitud) debían aplicarse de igual forma independientemente del riesgo del tratamiento, aunque se podía tener en cuenta que estos mismos principios han permitido siempre una modulación (con el uso de términos como adecuado, apropiado, razonable, necesario en artículo 6 y 7 Directiva 95/46/CE). *Ibídem.*

[1651] D.J. WEITZNER, H. ABELSON, T. BERNERS-LEE, J. FEIGENBAUM, J. HENDLER y G.J. SUSSMAN, "*Information Accountability*", *Communications of the ACM, op. cit.*, págs. 82 a 87. También desde el Foro Económico Mundial, se propugnaba un nuevo enfoque mediante el que se entendía que, por ejemplo, solicitar consentimiento para tratar datos había devenido una fórmula anacrónica y era preferible poner al alcance de los titulares de los datos herramientas para que pudieran controlar el uso de sus datos. *Unlocking the value of personal data: from collection to usage, World Economic Forum, op. cit.* pág. 18.

[1652] Es muy ilustrativo un ejemplo que se cita en el que una madre tiene un niño con una enfermedad crónica y busca información sobre la misma en Internet, compra libros, participa en foros. Cuando se presenta a una oferta de trabajo la rechazan y sospecha que es porque han podido acceder a la información de su actividad en Internet. Los autores subrayan que, en vez de incidir en si las empresas titulares de las web a las que ha accedido la madre han protegido la información, donde debería orientarse el foco es en la decisión de quien ofertaba el empleo de rechazarla en virtud de esa información. Por tanto, lo que verdaderamente daña a esta persona es la decisión adoptada en función de la información, el uso que se hace de la misma. *Ibídem.*

[1653] *Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, 14/EN WP 221, 16.9.2014, Article 29 Data Protection Working Party*.

Según el GA29, no había razón que llevara a decir que estos principios no son válidos y apropiados para el desarrollo del *big data*[1654].

Por otro lado, el GA29 recordó que, aunque haya diferentes niveles de aplicación de las obligaciones derivadas de la *accountability*, que dependerán del riesgo de la operación de tratamiento, los responsables siempre deberán responder del cumplimiento de sus obligaciones, en materia de protección de datos[1655]. Estas manifestaciones que tuvo que realizar el GA29, de nuevo, denotan el choque entre el sistema jurídico anglosajón y el continental.

El primero tiene una aproximación más pragmática, de forma que se fundamenta en la autorregulación de los operadores y en la protección *ex post* frente a los daños ocasionados por incumplimientos de esos operadores. La autorregulación incluye metodologías en las que los propios sujetos obligados son los que adaptan las medidas a sus características. Por eso, se adoptan métodos como el de la evaluación de riesgos. Cuando introducimos esos métodos en nuestro sistema jurídico hay que tener cuidado con el encaje que se realice y que no se rebaje el nivel de protección de los derechos fundamentales, núcleo del mismo. No se puede olvidar que lo que pretende nuestro sistema es obligar a los operadores con lo que establecen las leyes, de forma que hay principios como el de licitud que obligan al operador a tener una base jurídica legítima para poder tratar datos. Por tanto, no se confía en la autolimitación que puede llevar a cabo el operador en los usos de los datos.

El Consejo UE ha modificado el precepto pero los cambios más relevantes afectan a la introducción de la posibilidad de utilizar códigos de conducta y mecanismos de certificación para demostrar el cumplimiento de esta obligación (art. 30.2bis PCJ-RGPD) y a la inclusión de la obligación de confidencialidad en este precepto (art. 30.2ter PCJ-RGPD). Esta obligación es la que se refiere a la necesidad de que las personas autorizadas por el responsable y el encargado a acceder a los datos, los traten de acuerdo con las instrucciones de estos.

[1654] *Ibídem*, pág. 2.
[1655] *Statement on the role of a risk-based approach in data protection legal frameworks, op. cit.*, pág. 3.

f. Notificación de violaciones de datos

La incorporación de esta obligación supone la generalización de la misma para todos los responsables del tratamiento, ya que actualmente existe esta obligación, de forma sectorial, para los prestadores de servicios de comunicaciones electrónicas en el marco de la Directiva 2002/58/CE[1656]. Respecto a este deber de notificación sectorial, con el fin de asegurar un procedimiento uniforme en toda la UE, para realizar la notificación, se aprobó un reglamento europeo que lo regula[1657].

La violación de datos personales se define en la propuesta de la Comisión, como "toda violación de la seguridad que ocasione la destrucción accidental o ilícita, la pérdida, alteración, comunicación no autorizada o el acceso a datos personales transmitidos, conservados o tratados de otra forma" (art. 4.9 PCE-RGPD). La obligación de comunicar estas violaciones de datos[1658], contribuye a la transparencia en el tratamiento de datos de cara al interesado y permite que este pueda tener el control sobre lo que sucede con sus datos. No cabe duda la relevancia que conlleva un fallo de seguridad en el contexto de Internet, donde los datos pueden quedar expuestos a la vista de todo el mundo.

Se ha asignado la obligación al responsable que debe realizar una doble notificación a las autoridades de control y a los afectados por el incidente (arts. 31 y 32 PCE-RGPD). El Consejo UE ha reducido el alcance de la obligación respecto a los textos de la Comisión y el Parlamento. De forma que, en el caso de la notificación a la autoridad de control, los textos de la Comisión y el Parlamento establecen la obligatoriedad, en cualquier caso, cuando se produzca una violación. El Consejo UE, en cambio, matiza que sólo será obligatorio cuando sea probable que vaya a causar un alto riesgo para los derechos y libertades del interesado.

[1656] Esta obligación proviene también del sistema anglosajón, razón por la que conocemos a través de los medios de comunicación importantes problemas de seguridad. Así, la embajada estadounidense manifestó su apoyo al establecimiento de esta obligación que, tal como indicaba, se prevé en 47 Estados de ese país, así como en algunas de las leyes federales. De hecho, es un ejemplo de la influencia que EEUU tuvo en la preparación del borrador de reglamento. De esta forma, la embajada criticó el plazo para notificar que era de veinticuatro horas en el texto inicial, plazo que se amplió, como veremos. Nota de la Embajada de EEUU de enero de 2012, *op.cit.*.

[1657] Reglamento (UE) nº 611/2013 de 24 de junio de 2013 relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas, DO L 173, de 26.6.2013.

[1658] La traducción de "*personal data breach*" por "violaciones de datos" es ciertamente desafortunada.

Del mismo modo, en el caso de la notificación a los interesados, la Comisión y el Parlamento exigen que se produzca cuando sea probable que se afecte negativamente la protección de los datos o los derechos o los intereses legítimos[1659]. El Consejo UE dispone, sin embargo, que la notificación se realice si es probable que se produzca un alto riesgo para los derechos y libertades de los interesados.

El plazo inicial previsto para realizar esta notificación era de 24 horas, pero se amplió en el texto parlamentario y en el del Consejo UE a 72 horas y se permitió que se realizara por fases (art. 31.3 y Considerando 67 PPE-RGPD y art. 31.1 y .3bis PCJ-RGPD). El responsable tiene la obligación de documentar las violaciones, de forma que permita a la autoridad de control el control del cumplimiento del precepto (art. 31.4 PCE-RGPD).

Hay que tener en cuenta que uno de los factores que pueden incentivar que las organizaciones cumplan con las medidas de seguridad es el problema que una incidencia puede suponer para la confianza que los clientes o usuarios tengan en sus sistemas. La buena reputación, la imagen que una organización tiene frente a sus clientes o usuarios es, por tanto, un claro incentivo para la adopción de estas medidas en un contexto en el que, como ya se ha indicado, los modelos de negocio y de gestión se asientan en la tecnología, proclive a incidencias y ataques que pueden tener graves consecuencias para la protección de datos.

Estos factores se han tenido en cuenta y, así, el responsable podrá evitar la notificación al interesado de la violación, si demuestra a la autoridad de control que ha implementado medidas de protección tecnológica apropiadas, que hacen ininteligibles los datos para cualquier persona no autorizada (art. 32.3 PCE-RGPD). Es decir, si se han aplicado, por ejemplo, tecnologías de cifrado a los datos se evitará esta notificación.

El Consejo UE ha ampliado los supuestos en los que no será necesario notificar a los interesados la violación (art. 32.3 PCJ-RGPD). Se ha excepcionado la notificación si el responsable ha adoptado, posteriormente, medidas que hagan desaparecer la probabilidad de que se materialice el alto riesgo, en la afectación de los derechos, o si la

[1659] La referencia a los intereses legítimos la añade el Parlamento (art. 32.1 PPE-RGPD).

comunicación supusiera una tarea desproporcionada, o si afectase negativamente a un interés público esencial. Estos supuestos revisten una gran indeterminación, por lo que pueden favorecer la inseguridad jurídica.

2.2.3. Una pluralidad de participantes

Fruto de la revisión que se realizó del contexto tecnológico, se concluyó que los modelos de negocio propician la participación de una multitud de actores, respecto a los que es difícil dirimir responsabilidades. La idea de que un solo responsable deberá responder no casa bien con esta realidad. En aras de una aproximación pragmática de este problema, es necesario que se articulen mecanismos para garantizar que todos los implicados contribuirán a cumplir con lo establecido en la normativa y, al mismo tiempo, que aseguren que se responderá ante un posible incumplimiento.

Estas necesidades han implicado que, en el reglamento se de relevancia a otros sujetos que intervendrán en asegurar el cumplimiento de sus previsiones. Al lado del responsable, el encargado adquiere un papel esencial que se ve correspondido con una asignación clara de responsabilidad. Las situaciones de corresponsabilidad se regulan y se refuerzan otras figuras que coadyuvan en el cumplimiento: el representante y el delegado de protección de datos.

a. El encargado del tratamiento

Respecto a las obligaciones que tiene el responsable que decide contratar un encargado del tratamiento, se refuerza la exigencia al responsable respecto a la elección y control del encargado. De esta forma se incide en que el encargado elegido debe ofrecer garantías suficientes para cumplir con las medidas técnicas y organizativas que deben asegurar el cumplimiento del reglamento (art. 26.1 PCE-RGPD). Pero el responsable, no solo debe elegir bien, sino que debe velar porque el encargado cumpla con estas medidas. Esta responsabilidad *in vigilando* fue eliminada por el Consejo UE.

Tanto el Parlamento, como el Consejo UE, introdujeron la posibilidad de que estas garantías suficientes se pudieran demostrar con el cumplimiento de códigos de conducta o mecanismos de certificación (arts. 26.3bis PPE-RGPD y 26.2bis bis PCJ-RGPD).

Tanto el responsable, como el encargado, están obligados a suscribir un contrato que incluirá las obligaciones del encargado que se establecen en el reglamento (art. 26.2 PCE-RGPD)[1660]. Respecto a este contrato, el Consejo UE estableció la posibilidad de utilizar cláusulas tipo que podrían elaborar la Comisión, las autoridades de control o provenir de los mecanismos de certificación (art. 26.2bis ter, .2ter y .2quater PCJ-RGPD). Asimismo, se establece una obligación para ambos de documentar por escrito las instrucciones del responsable al encargado y las obligaciones de éste (art. 26.3 PCE-RGPD).

El Parlamento dispuso que el responsable y el encargado pudieran determinar libremente sus papeles y tareas, respecto a los requisitos del reglamento. Debe entenderse que esto no puede implicar, en ningún caso, que el encargado determine los fines y los medios del tratamiento, ya que eso podría ocasionar que se pudiera articular la responsabilidad y desvirtuaría los conceptos.

i. Las obligaciones del encargado del tratamiento

El núcleo de obligaciones que tiene el encargado respecto al responsable está en el artículo 26.2 PCE-RGPD. El encargado deberá tratar los datos personales, de acuerdo con las instrucciones del responsable. Tanto el Parlamento, como el Consejo UE añadieron que también podría tratar datos si la legislación de la Unión o del Estado miembro lo exigiera[1661]. Se trata de hallar en la ley la fuente de legitimación para tratar datos. Como ya vimos, habrá que analizar si esa obligación legal pudiera convertir al encargado en responsable, por atribuirle la capacidad de determinar los fines o medios del tratamiento o si permite que mantenga su cualidad de encargado del tratamiento.

El encargado sólo empleará personal que se haya comprometido a respetar la confidencialidad o esté sujeto a una obligación legal de confidencialidad[1662] y cumplirá con las medidas de seguridad del artículo 30 PCE-RGPD. Asimismo, deberá ayudar al

[1660] El Consejo UE estableció que el contrato debía fijar "el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados afectados y los derechos del responsable" (art. 26.2 PCJ-RGPD).
[1661] Como se verá, todas las alusiones a la legislación como fuente de obligaciones se refieren a leyes de la UE o de los Estados miembros, lo que deja fuera la posibilidad de acudir a legislaciones de otros países.
[1662] Esta obligación fue eliminada por el Consejo UE.

responsable, en el cumplimiento de su obligación de dar curso a las solicitudes de ejercicio de derechos de los interesados, y de las obligaciones de los artículos 30 a 34 PCE-RGPD[1663].

Para poder subcontratar, el encargado del tratamiento necesitará la autorización previa del responsable del tratamiento. El Parlamento permitió que se pudiera establecer otro modo para permitir la subcontratación sin concretar cual (art. 26.2.d) PPE-RGPD). El Consejo UE desarrolló un poco más la subcontratación, de forma que incluyó la necesidad de que el encargado del tratamiento suscribiera un contrato con el subencargado, similar al establecido para responsable y encargado (art. 26.2bis PCJ-RGPD).

El encargado devolverá los resultados del tratamiento al responsable al término de éste y se abstendrá de tratar esos datos. El Parlamento añadió que el encargado debía borrar las copias, a no ser que la legislación de la Unión o de los Estados miembros exigiera conservarlas. El Consejo UE indicó que a elección del responsable, el encargado debería devolver o suprimir los datos, salvo que la legislación le obligara a conservar los datos[1664].

El encargado pondrá a disposición del responsable y de la autoridad de control la información para demostrar el cumplimiento de estas obligaciones del artículo 26 PCE-RGPD (art. 26.2.h) PCE-RGPD). Tanto el Parlamento, como el Consejo UE modificaron esta obligación, de forma que el encargado solo debiera poner esta información a disposición del responsable y pudiera efectuar inspecciones *in situ*, según el Parlamento o auditorías, según el Consejo UE. Además, el Consejo UE incluyó la obligación de que el encargado informara al responsable si considerara que una instrucción del responsable vulnerara el reglamento o la legislación de protección de datos de la Unión o de los Estados miembros.

Sin embargo, las obligaciones del encargado no se limitan a estas del artículo 26.2 PCE-RGPD sino que, como hemos visto al revisar las del responsable, también aparece

[1663] Es decir, las obligaciones relativas a la seguridad, notificación de violaciones de datos, evaluación de impacto y autorización y consulta previas.
[1664] Estas disposiciones, al igual que toda esta regulación es muy similar a la española.

en la mayoría de ellas, por lo que se le adjudica, sin duda, un papel relevante en su cumplimiento.

ii. La activación de la responsabilidad del encargado

Por último, hay que mencionar que, independientemente de la responsabilidad civil que veremos posteriormente, en la propuesta de la Comisión y en el texto del Parlamento se han previsto unas reglas que permitirán la atribución de responsabilidad al encargado. De esta forma, la Comisión estableció que, si el encargado del tratamiento trataba datos, sin seguir las instrucciones del responsable, el encargado sería considerado responsable del tratamiento y estaría sujeto a las normas aplicables a los corresponsables (art. 26.4 PCE-RGPD). El Parlamento añadió que el encargado también sería responsable si se convirtiera en parte determinante respecto a los fines y medios del tratamiento.

Por tanto, se articula una activación de la responsabilidad del encargado similar a la que se encuentra en la LOPD, en la medida en que cuando el encargado no sigue las instrucciones del responsable se convierte en responsable (art. 12.4 LOPD). Sin embargo, en los textos de la Comisión y del Parlamento, se reconduce al régimen de corresponsabilidad, de forma que si no hay acuerdo entre los corresponsables (en este caso entre el responsable y el encargado que se ha convertido en responsable) estos responderían solidariamente. Hay que decir que el Consejo UE suprimió esta referencia a la responsabilidad del encargado pero, por otro lado, estableció la responsabilidad del encargado principal, respecto al incumplimiento del subencargado (art. 26.2bis PCJ-RGPD).

Esta supresión de la responsabilidad podría deberse a que el Consejo UE ha previsto en su régimen sancionador, de forma expresa, que se sancionará tanto al responsable como al encargado. Si bien, en el texto de la Comisión, aunque el sujeto infractor se defina de forma neutra, también debe comprender al encargado del tratamiento, ya que, algunas infracciones se refieren claramente a este[1665].

[1665] La propuesta de la Comisión establecía una multa de hasta 1.000.000 € o de hasta el 2% del volumen de negocios anual, para todo aquel que, de forma deliberada o por negligencia tratara o instruyera el tratamiento de datos incumpliendo las obligaciones relativas al tratamiento por cuenta de un responsable del tratamiento comprendidas en los artículos 26 y 27 (art. 79.6.g) PCE-RGPD). Esta infracción se reproduce en el texto del Consejo UE, aunque como he indicado, la multa se podrá imponer al responsable o al

Otro aspecto que ya se reflejaba en la Directiva 95/46/CE respecto al encargado y a las personas sometidas a la autoridad del responsable y del encargado, era la posibilidad de desviarse del encargo del responsable cuando un imperativo legal así lo dispusiera. En los textos de la Comisión y del Parlamento esta vía de escape también se ha previsto en un precepto que ha permanecido sin cambios (art. 27 PCE-RGPD). Además se ha reforzado para el encargado del tratamiento, en la resolución del Parlamento, como ya se ha visto, al indicar que seguirá las instrucciones del responsable, a menos que la legislación exija lo contrario (art. 26.2.a) y g) PPE-RGPD).

Asimismo, el Consejo UE, que eliminó el artículo 27 PCE-RGPD, incluyó esta vía de escape en la regulación del encargado (art. 26.2.a) y g) PCJ-RGPD) y en la obligación de seguridad respecto a las personas que actúan bajo la autoridad del responsable o del encargado (art. 30.2ter PCJ-RGPD). También se añadió que si el encargado debía actuar en virtud de una obligación legal, tendría que informar al responsable de esta exigencia, salvo si la disposición legal le prohibía dicha información por motivos importantes de interés público.

La utilización de esta vía para no atender las instrucciones del responsable plantea la duda de si implicaría que se aplique el apartado 4 del artículo 26 PRGPD, que activaría la responsabilidad del encargado[1666]. Por otro lado, parece más adecuada la previsión del Consejo UE al disponer que el encargado informe en caso de tener una obligación legal que le obliga a tratar datos en contra de las instrucciones del responsable. De esta forma, podríamos considerar que el responsable no deja de tener el control, porque podrá decidir si quiere seguir con el encargo o no. Y es que habría que examinar si la obligación legal implica que el encargado determine los fines o los medios del tratamiento.

La resolución del Parlamento contempla un supuesto que exonera al encargado de cumplir con el reglamento. Con el fin de evitar que se proceda al tratamiento de datos, con el único fin de cumplir lo previsto en el reglamento, se prohibía al responsable el

encargado del tratamiento cuando trate o instruya el tratamiento de datos personales incumpliendo el artículo 26 (art. 79bis.dquater PCJ-RGDP).

[1666] También se plantea la duda respecto a las personas sometidas a la autoridad de responsable y encargado que, según el artículo 27 PCE-RGPD, y tal como se preveía en la Directiva 95/46/CE también podían desviarse de su deber de seguir los dictados de estos si la legislación así lo disponía.

tratamiento de información adicional del interesado con el único fin de identificarlo para cumplir con el reglamento, y ello si los datos que trataba el responsable o el encargado, no le permitían identificarlo, directa o indirectamente o constituían datos seudónimos (art. 10.1 PPE-RGPD). Pues bien, a continuación este precepto establecía que cuando el encargado no pudiera cumplir alguna de las disposiciones del reglamento debido a esta prohibición se le dispensaría de cumplirla (art. 10.2 PPE-RGPD). El Consejo UE no contempló esta previsión relativa al encargado.

En todo caso, estas disposiciones denotan el incremento de rasgos de independencia en la figura del encargado que pueden hacer aún más difícil delimitar cuando estaremos ante un responsable o un encargado. También es cierto que al atribuirse responsabilidad al encargado, ya no es tan relevante determinar quién es el responsable, como cuando era el único sujeto que podía responder ante el interesado. Este reparto del poder entre ambos sujetos obligados puede conllevar el riesgo de que los roles sean aún más difíciles de predecir y de asignar. Esto agravaría aún más las debilidades del concepto de responsable y exigirán un esfuerzo por parte de las autoridades para clarificarlo.

b. La corresponsabilidad

En la línea de lo que señaló el GA29, en referencia a los supuestos de corresponsabilidad, en los que estimaba que era mejor otorgar a los corresponsables una cierta flexibilidad en el reparto de obligaciones y responsabilidades, se ha incluido una regulación en el reglamento[1667]. Así, la Comisión estableció que cuando un responsable determinara, conjuntamente con otros, los fines, las condiciones y los medios del tratamiento, los corresponsables dispondrían, por mutuo acuerdo, sus responsabilidades en el cumplimiento de las obligaciones del reglamento y en especial, respecto al ejercicio de derechos de los interesados (art. 24 PCE-RGPD)[1668].

El Parlamento añadió que en este acuerdo se reflejarían los papeles de los corresponsables y su relación con los interesados (art. 24 PPE-RGPD). El contenido

[1667] Ver Capítulo II.
[1668] Hay que tener en cuenta que la Comisión, en su propuesta había incluido el término “condiciones”, como uno de los aspectos sobre los que tenía capacidad de determinación el responsable.

esencial de este acuerdo se pondría a disposición de los interesados. Si la responsabilidad no pudiera determinarse, los responsables responderían solidariamente.

El Consejo UE, respecto a la propuesta de la Comisión, además de dirigir la determinación de las responsabilidades a cumplir, especialmente, lo relativo al ejercicio de derechos, incidió también en el cumplimiento del deber de información (art. 24.1 PCJ-RGPD). Añadió una salvedad respecto a esta determinación de responsabilidad, si la legislación de la UE o del Estado miembro, estableciera las responsabilidades. Como el Parlamento, el Consejo UE exigió que se pusieran a disposición de los interesados los aspectos esenciales del acuerdo, pero añadió que, se designaría en el mismo, al responsable que actuaría como punto único de contacto para el ejercicio de derechos (art. 24.1 y 3 PCJ-RGPD)[1669].

Si bien es un paso importante el de regular la corresponsabilidad, puede ser difícil en situaciones, como las que se describían, en el entorno tecnológico, en las que, en ocasiones, los corresponsables no se han puesto de acuerdo para realizar el tratamiento. Por otro lado, las situaciones no son simétricas y, tal como indicaba el GA29, pese a introducirse la flexibilidad en el acuerdo, ésta debe servir a un cumplimiento más eficiente y no para configurar el juego de responsabilidades para que beneficie a unos corresponsables, en perjuicio de otros, según convenga.

Otra dificultad que me plantea esta regulación es que, al indicar, como en la definición del responsable fines "y" medios, parece que los corresponsables deben decidir sobre ambos aspectos, lo que ya he indicado que no sería práctico, puesto que cualquier sujeto que determine los fines o los medios esenciales, debe ser considerado responsable.

Por último, determinar cuando estamos ante un supuesto de corresponsabilidad, exige previamente identificar a estos sujetos como responsables y entender, por tanto, que no son encargados del tratamiento. La corresponsabilidad supone un incremento en la madurez de la regulación. Sin embargo, si no aplicamos de forma consistente los

[1669] Se añade, de forma bastane confusa que los interesados podrían ejercer sus derechos ante cada uno de los corresponsables, salvo si se les hubiera informado del corresponsable que se hará responsable, a no ser que el acuerdo se considerara abusivo, de acuerdo con la legislación de la UE o de un Estado miembro (art. 24.3 PCJ-RGPD).

conceptos, esta madurez podría constituir un espejismo y conducir a más inseguridad jurídica y a la arbitrariedad en la utilización de las nociones.

c. El delegado de protección de datos

Esta figura vendría a sustituir al encargado de protección de datos personales, establecido en el artículo 18 Directiva 95/46/CE. Hay que recordar que la figura de la Directiva 95/46/CE era de acogimiento voluntario por parte de los Estados miembros, por lo que sólo en algunas leyes nacionales se adoptó. Además lo que pretendía era eliminar o simplificar la obligación de notificación a la autoridad de control, obligación que no se ha mantenido en el reglamento, sustituida por la de consultas ya indicada.

El delegado de protección de datos instituido por el reglamento adquiere una mayor relevancia, especialmente en los textos de la Comisión y el Parlamento, en los que su designación deviene obligatoria en los supuestos establecidos. El Consejo UE, sin embargo, deja a la voluntad del legislador europeo o nacional que establezca su designación como obligatoria o si los responsables o encargados quieren nombrarlo (art. 35.1 PCJ-RGPD).

La Comisión y el Parlamento obligaban al responsable y al encargado a designarlo cuando el tratamiento lo llevara a cabo una autoridad u organismo público y si las actividades principales del responsable o del encargado del tratamiento consistían en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requerían un seguimiento periódico y sistemático de los interesados.

La Comisión también dispuso la obligatoriedad de designarlo cuando el tratamiento lo llevara a cabo una empresa que empleara a doscientas cincuenta personas o más. En cambio el Parlamento modificó este supuesto para referirse a cuando el tratamiento lo llevara a cabo una persona jurídica con respecto a más de cinco mil interesados, durante un periodo consecutivo de doce meses.

Por último, el Parlamento añadió otro supuesto de designación obligatoria del delegado, cuando las actividades principales del responsable o del encargado del tratamiento consistieran en el tratamiento de categorías especiales de datos con arreglo al

artículo 9.1 PPE-RGPD[1670], datos de localización, o datos relativos a niños, o a empleados en ficheros a gran escala.

Esta figura, como ya se comentó reúne algunas características de la *accountability*, ya que supone designar una persona concreta que velará porque se cumpla el reglamento. Este delegado, según los tres textos, informará directamente a la dirección ejecutiva del responsable o el encargado (art. 36.2 PCE-RGPD). Incluso, el texto del Parlamento añadió que se tendrá que nombrar, a estos efectos, a un miembro de la dirección ejecutiva que será el responsable de cumplir con el reglamento (art. 36.2 PPE-RGPD)[1671].

Asimismo, la designación del delegado responde al objetivo de transparencia, de forma que todos los textos exigen la comunicación de la designación a la autoridad de control y al público (art. 35.9 PCE-RGPD). Además, la Comisión y el Parlamento han incluido el derecho de los interesados a contactar con el delegado (art. 35.10 PCE-RGPD), mientras que el Consejo UE rebaja esta previsión al indicar que "podrán" contactarlo (art. 35.10 PCJ-RGPD).

Se exige que el delegado sea designado, en virtud de sus cualificaciones profesionales, conocimientos especializados en la legislación y prácticas de protección de datos, y a su capacidad para ejecutar las tareas que se establecen en el reglamento (art. 35.5 PCE-RGPD)[1672]. Podrá ser un empleado de la organización o un proveedor de servicios externos (art. 35.8 PCE-RGPD). En caso de grupos de empresas o de administraciones públicas, se permite que se puedan nombrar un delegado para varias entidades (art. 35.2 y .3 PCE-RGPD).

[1670] Estos datos serían los que revelen el origen étnico o racial, las opiniones políticas, la religión o las creencias filosóficas, la orientación sexual o la identidad de género, la afiliación y las actividades sindicales, así como el tratamiento de datos genéticos o biométricos o de datos relativos a la salud, la vida sexual, las sanciones administrativas, las sentencias, los delitos o las sospechas de delito, las condenas penales o las medidas de seguridad afines (art. 9.1 PPE-RGPD).

[1671] Se cumpliría así con la característica de la *accountability* que exigía implicar a la dirección de la empresa.

[1672] De forma resumida y según el texto del Parlamento, que es el que ha incorporado la lista más extensa, son: asesorar al responsable o al encargado sobre sus obligaciones, supervisar la aplicación de las políticas en materia de protección de datos, supervisar la aplicación del reglamento, velar por la conservación de la documentación, supervisar la comunicación de violaciones de datos, supervisar la realización de evaluaciones de impacto y presentación de consultas previas, supervisar respuestas y cooperar con las autoridades de control, actuar como punto de contacto para la autoridad de control, informar a los representantes de los trabajadores sobre el tratamiento (art. 37 PPE-RGPD).

Asimismo se establece la necesidad de que cuente con la debida independencia y que sus funciones profesionales sean compatibles con sus funciones como delegado de protección de datos (art. 36.2 PCE-RGPD). También se le deben procurar los medios y recursos suficientes para desempeñar sus tareas (art. 36.3 PCE-RGPD).

El delegado sólo podrá ser destituido durante su mandato si deja de cumplir las condiciones requeridas para el ejercicio de sus funciones (art. 35.7 PCE-RGPD). La Comisión preveía un mandato de dos años (art. 35.7 PCE-RGPD), que el Parlamento modificó por uno de cuatro años si es empleado y de dos años si es prestador de servicios externo (art. 35.7 PPE-RGPD), aunque se pueden renovar los mandatos en ambos textos. El Consejo UE no establece la duración mínima del mandato y permite la destitución, además de en el caso mencionado, si así lo establece la legislación del Estado miembro por motivos graves que justifiquen la destitución de un empleado o funcionario (art. 35.7 PCJ-RGPD).

d. El representante del responsable

En los casos en los que se aplique el reglamento a responsables que no están establecidos en la UE, según el criterio de aplicación establecido en el artículo 3.2 PCE-RGPD, estos responsables están obligados a designar a un representante.

La definición de representante es toda persona física o jurídica establecida en la Unión que, designada expresamente por el responsable del tratamiento, actúe en lugar del responsable, en lo que respecta a las obligaciones de éste último, en virtud del reglamento (art. 4.14 PCE-RGPD)[1673]. Consecuentemente, con esta definición el representante no debería contar con obligaciones propias, sino que tendría las obligaciones que el reglamento estableciera para el responsable. Sin embargo se le han asignado algunas en el texto, especialmente dirigidas a la colaboración con las autoridades de control[1674].

[1673] Se suaviza la definición en el trámite parlamentario, ya que en la versión inicial del texto se había establecido, en vez de que representaba al responsable, que actuaba en lugar del mismo y a quien podía dirigirse cualquier autoridad u organismo en lugar del responsable, en lo que respecta a las obligaciones del reglamento. El Consejo UE especifica que la designación debe ser por escrito (art. 4.14, 25.3bis y Considerando 63 PCJ-RGPD).

[1674] Se cita expresamente al representante como sujeto obligado en la PCE-RGPD en el artículo 28.1 (obligación de conservar la documentación relativa a las operaciones de tratamiento), artículo 28.3 (puesta a disposición de la autoridad de control de documentación) y artículo 29.1 (cooperación con autoridades de

Según los textos de la Comisión y del Consejo UE, este representante debe hallarse en uno de los Estados miembros donde residan los interesados cuyos datos son objeto del tratamiento, en los dos supuestos que activan la aplicación del reglamento (art. 25.3 PCE-RGPD). El Parlamento optó, sin embargo, porque estuviera en uno de los Estados miembros donde tenga lugar la oferta de bienes o servicios, por parte del responsable a los interesados o donde se efectúe el control de su conducta (art. 25.3 PPE-RGPD).

Para llevar a cabo esa función, se incluyen los datos del representante entre la información que debe proporcionarse al interesado cuando se recojan sus datos (art. 14.1.a PCE-RGPD).

Sin embargo, esta obligación de designar representante cuenta con algunas excepciones que se refieren a cuando el responsable esté establecido en un país con nivel adecuado de protección, cuando sea una empresa que emplee a menos de doscientas cincuenta personas, cuando se trate de una autoridad u organismo público o cuando la oferta de bienes o servicios sea ocasional (art. 25.2 PCE-RGPD). El Parlamento matizó estas excepciones, principalmente, para que no se aplicaran a datos de categorías especiales (art. 25.2 PPE-RGPD). El Consejo UE sólo mantuvo dos excepciones, para el caso de que el responsable fuera una autoridad u organismo público, o si las operaciones de tratamiento tuvieran carácter ocasional y pocas probabilidades de dar lugar a un riesgo para los derechos de las personas (art. 25.2 PCJ-RGPD).

Si bien se mantiene la alusión que se hacía en la Directiva 95/46/CE a que la designación de este representante no obsta para que se puedan ejercitar las acciones legales contra el responsable del tratamiento (art. 25.4 PCE-RGPD) se establece que la sanción se podrá imponer a este representante (art. 78.2 PCE-RGPD). El Consejo UE eliminó esta alusión a la imposición de la sanción, pero incluyó en el preámbulo que el

---

control), artículo 53.1.c) (obligación de entregar información a las autoridades de control). En la PPE-RGPD se incluyen las siguientes obligaciones para el representante: artículo 33.3.ter (obligación de poner a disposición de la autoridad de control la documentación de la evaluación de impacto), artículo 33bis.4 (obligación de poner a disposición de la autoridad de control la documentación relativa a la revisión de cumplimiento), artículo 43bis (obligación de comunicar y obtener autorización de la autoridad de control en caso de que una sentencia de un tribunal o autoridad administrativa de un tercer país exijan que haga público los datos).

representante podría estar sujeto a medidas coercitivas, en caso de incumplimiento del responsable (Considerando 63 PCJ-RGPD).

2.3. Las obligaciones derivadas de los principios relativos al tratamiento de datos, de los derechos de los interesados y de la regulación de las transferencias internacionales de datos

2.3.1. Las obligaciones derivadas de los principios relativos al tratamiento de datos

Los principios que se aplicarán al tratamiento de datos se encuentran en el artículo 5 PCE-RGPD. Se trata de los antiguos principios de calidad del artículo 6 Directiva 95/46/CE, a los que se ha añadido la transparencia y la rendición de cuentas. En trámite parlamentario, se les han atribuido unos títulos y se les ha añadido otros dos: efectividad e integridad. El principio de efectividad persigue que los datos sean tratados, de forma que permita a los interesados poder ejercer sus derechos. El principio de integridad es que los datos estén protegidos, por lo que corresponde a la obligación de seguridad.

Los datos deberán ser tratados, de acuerdo con estos principios relativos al tratamiento de datos que son: licitud, lealtad y transparencia; limitación de los fines; minimización de los datos; exactitud; minimización de la conservación; efectividad; integridad y *accountability* (rendición de cuentas). La observancia de estos principios es una obligación que considero implícita para el responsable, ya que no se asigna a este expresamente (con excepción del de rendición de cuentas de asignación expresa, como ya se ha indicado).

El Consejo UE, en su orientación general, eliminó el principio de *accountability* de este listado, pero añadió un principio que se refiere a la garantía de la seguridad de los datos (art. 5.1.ee) PCJ-RGPD). Respecto al principio de limitación de fines se incluyó, de forma similar a como sucedía en la Directiva 95/46/CE, la posibilidad de tratar datos con fines científicos, estadísticos o históricos o para archivo en interés público, sin que ello se considere tratar datos para fines incompatibles (art. 5.1.b) PCJ-RGPD). Asimismo, con estos mismos fines, se dispuso la posibilidad de conservar los datos durante períodos más

largos, en el marco del principio de minimización de la conservación (art. 5.1.e) PCJ-RGPD)[1675].

En desarrollo del principio de licitud, se establece la obligación, que también sería de asignación implícita al responsable, de aplicar alguno de los supuestos establecidos para poder realizar un tratamiento de datos (corresponderían a los supuestos de legitimación del tratamiento del artículo 7 Directiva 95/46/CE). Así, se mantienen básicamente los mismos supuestos de la Directiva 95/46/CE, si bien se incorporan algunas novedades[1676].

Se introduce una definición de lo que se considera consentimiento, de forma que la propuesta de la Comisión y la resolución del Parlamento reforzaban este requisito, al exigir que la manifestación de voluntad fuera explícita (art. 4.8 PCE-RGPD). Por tanto, quedaba claro que no cabía el consentimiento tácito, como, por ejemplo se admitía en la normativa española[1677]. Sin embargo, en la orientación del Consejo UE se elimina esta característica (art. 4.8 PCJ-RGPD).

También se regulan las condiciones del consentimiento (art. 7 PCE-RGPD). Así se dispone en los tres textos que la carga de la prueba sobre el consentimiento será asumida por el responsable del tratamiento y se establece el derecho a retirar el consentimiento aunque sin efectos retroactivos. Si el consentimiento se otorga en el contexto de una declaración escrita que se refiera a otros asuntos, debe requerirse de forma que se distinga bien de esos otros asuntos.

Se incide en que el consentimiento debe ser libre, por lo que sólo constituirá una base jurídica válida para tratar datos si la persona tiene libertad de elección, lo que

[1675] Esta posibilidad de tratar y conservar datos con estos fines se efectuará, tal como señala el precepto, de acuerdo con el artículo 83 PCJ-RGPD, que establece excepciones respecto al cumplimiento de algunos de los preceptos del Reglamento que pueden habilitar los Estados miembros y la UE si aplican las debidas garantías.

[1676] Los supuestos que habilitarían el tratamiento, de forma resumida serían: si el interesado ha dado su consentimiento; si el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado; si el tratamiento es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto un responsable; el tratamiento es necesario para proteger intereses vitales del interesado; el tratamiento es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable; el tratamiento es necesario para la satisfacción de un interés legítimo perseguido por el responsable, siempre que no prevalezcan los derechos y libertades del interesado (art. 6 PCE-RGPD).

[1677] Ver Capítulo III.

implica que puede denegar o retirar el consentimiento sin sufrir perjuicios[1678]. En la parte de los Considerandos, las tres instituciones se refieren a la posibilidad de otorgar el consentimiento a través de Internet. Se acepta la selección de una casilla o cualquier declaración que indique claramente que se acepta el tratamiento (Considerando 25 PCE-RGPD). El Consejo UE, pese a no establecer el consentimiento explícito, sino inequívoco, también indica lo mismo, pero además añade que si fuera técnicamente posible también se podrá dar el consentimiento a través de los oportunos ajustes de un buscador o de otra aplicación (Considerando 25 PCJ-RGPD).

También hay que tener en cuenta una obligación de asignación expresa al responsable relacionada con el consentimiento. Así, el responsable deberá verificar el consentimiento que deben dar los padres o el representante legal de un menor de trece años para poder tratar datos de estos menores a los que oferte directamente bienes o servicios (art. 8.1 PCE-RGPD)[1679].

Respecto al supuesto relativo al interés legítimo, la Comisión sólo incluía el referido al responsable y no contemplaba la posibilidad de tratar los datos, en virtud del interés legítimo del tercero al que se comuniquen, como se establecía en la Directiva 95/46/CE (art. 7.f) Directiva 95/46/CE). Esta posibilidad se añadió en el texto del Parlamento y el Consejo UE (art. 6.1.f) PPE-RGPD y PCJ-RGPD). El Parlamento también incluyó que el tratamiento debía cumplir las expectativas razonables del interesado, sobre la base de su relación con el responsable del tratamiento. Evidentemente, se mantiene en todos los textos la necesaria prevalencia de este interés legítimo sobre el interés o los derechos y libertades fundamentales del interesado, que requiera protección de los datos personales, para que el responsable pueda tratar datos en virtud de su interés.

[1678] En la resolución del Parlamento, a modo de ejemplo se cita el caso en el que el responsable sea una autoridad pública cuando impone una obligación en virtud de sus poderes, lo que conlleva que no se pueda considerar que haya consentimiento libre o el uso de casillas ya marcadas que impliquen que el interesado debe modificarlas para oponerse al tratamiento (Considerando 33 PPE-RGPD). En el texto del Consejo UE, en cambio se indica que el consentimiento no será libre si existe un desequilibrio claro entre el interesado y el responsable (Considerando 34 PCJ-RGPD). Esta previsión se hallaba en la propuesta de la Comisión (art. 7.4 PCE-RGPD) pero el Consejo UE prefirió incluirlo en la parte de los Considerandos.

[1679] En los tres textos se refieren a que esta disposición no afectará a lo establecido por el derecho civil de los Estados miembros en materia de contratos (art. 8.2 PCE-RGPD). El Consejo UE no se refiere a ninguna edad mínima del menor, sino que remite a la legislación de la Unión o del Estado miembro para hallar los requisitos para considerar válido dicho consentimiento (art. 8.1 PCJ-RGPD).

La Comisión y el Parlamento establecieron que esta base jurídica no se aplicaría al tratamiento realizado por las autoridades públicas, en el ejercicio de sus funciones (art. 6.1.f) PCE-RGPD). El GA29 alertó a este respecto, ya que algunos tratamientos de datos personales, que realizan estas entidades podrían quedarse sin base jurídica[1680]. El Consejo UE eliminó este apartado (art. 6.1.f) PCJ-RGPD).

El GA29 también criticó la posibilidad que permitía la propuesta de la Comisión, de realizar un tratamiento de datos ulterior, aunque la finalidad fuera incompatible con aquella para la que se recogieron los datos, si se acudía a una base jurídica para legitimar el tratamiento (excepto la relativa al interés legítimo que no se admitiría) (art. 6.4 PCE-RGPD).

Hay que recordar que según el GA29, en la actual regulación esto no sería posible, ya que se exige que los artículos 6 y 7 Directiva 95/46/CE sean acumulativos y, por tanto, si una finalidad es incompatible no cabe aplicar una base jurídica, como si fuera un nuevo tratamiento de datos, porque eso iría en contra del espíritu del principio de finalidad[1681]. El Parlamento suprimió este apartado, pero el Consejo UE lo ha vuelto a introducir e incluso admite acudir a la base jurídica del interés legítimo, si se considera que este interés del responsable supera al del interesado (art. 6.4 PCJ-RGPD)[1682].

Otra obligación de asignación implícita al responsable es que no se podrá realizar un tratamiento de categorías especiales de datos, a no ser que concurran las condiciones establecidas (art. 9 PCE-RGPD). Las categorías especiales de datos que se contemplan en

[1680] El GA29 menciona tratamientos ligados a un mejor funcionamiento de las administraciones públicas que no serían estrictamente propios de la misión pública o del ejercicio del poder público. El GA29 hace referencia al Reglamento 45/2001, que no incluye ninguna base jurídica referida a la satisfacción del interés legítimo del responsable y lo que se ha hecho es interpretar de forma amplia la base jurídica que se incluye referida al interés público. De esta forma, el GA29 indica que, si se mantiene la disposición en el Reglamento, deberá optarse por seguir también una interpretación amplia del supuesto relativo al cumplimiento de la misión de interés público o inherente al ejercicio del poder público (art. 6.1.e) PCE-RGPD), para poder incluir estos tratamientos que se quedarían sin base jurídica. Otra opción que apunta el GA29 sería entender esta exclusión del artículo 6.1.f) PCE-RGPD de forma estricta y, por tanto, que sólo excluye aquellos tratamientos que estarían claramente incluidos en el artículo 6.1.e) PCE-RGPD, por lo que los tratamientos relativos al buen funcionamiento de las administraciones públicas se podrían incluir en la base jurídica del interés legítimo. *Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC op. cit.*, pág. 23.

[1681] *Opinion 3/2013 on purpose limitation, op. cit.*, págs. 36 a 37.

[1682] Por ello, el GA29 ha vuelto a insistir, de cara a influir en la negociación entre las instituciones, para eliminar este apartado. *Annex to letters in view of the trilogue: Core topics in view of the trilogue, 17.6.2015, Article 29 Working Party*, pág. 7.

el reglamento se han ampliado, respecto a la Directiva 95/46/CE, especialmente en la resolución del Parlamento, de forma que incluye: los datos que revelen el origen étnico o racial, las opiniones políticas, la religión o las creencias filosóficas, la orientación sexual o la identidad de género, la afiliación y las actividades sindicales y los datos genéticos o biométricos, los datos relativos a la salud y a la vida sexual (art. 9.1 PPE-RGPD). Además, se incorpora a la prohibición general de tratamiento, el de los datos de sanciones administrativas, las sentencias, delitos o sospechas de delitos, condenas penales o medidas de seguridad afines. En cambio, el Consejo UE sólo añade, respecto a los datos que incluía la Directiva 95/46/CE, los datos genéticos (art. 9.1 PCJ-RGPD).

Respecto a las excepciones a la prohibición de tratar estas categorías de datos, hay algunas variaciones. De esta forma, el consentimiento que permitía el tratamiento, en los textos de la Comisión y el Parlamento, ya no cuenta con el calificativo de explícito, puesto que este requisito se incluía en la definición de lo que se consideraba consentimiento. Sí se incluye esta característica en la orientación del Consejo UE (art. 9.2.a) PCJ-RGPD).

El Parlamento añadió otra excepción, para el caso en el que el tratamiento fuera necesario para el cumplimiento o la ejecución de un contrato, en el que el interesado fuera parte o para la adopción de medidas precontractuales a petición del interesado (art. 9.2.abis PPE-RGPD). Además se reforzó el supuesto del tratamiento necesario para cumplir una misión de interés público, que debía tener un "especial" interés público (art. 9.2.g PPE-RGPD).

El tratamiento de los datos relativos a sanciones administrativas, las sentencias, delitos, condenas penales o medidas de seguridad afines, además de ser realizado bajo supervisión de los poderes públicos, también se podrá realizar para cumplir una obligación jurídica o reglamentaria del interesado o para el desarrollo de una tarea por motivos importantes de interés público, siempre que lo autorice una legislación de la Unión o de los Estados miembros (art. 9.2.j PPE-RGPD)[1683].

[1683] Si bien se añade que el registro de condenas penales sólo se podrá llevar bajo el control de poderes públicos. Asimismo, hay que decir que no se incluye en esta previsión del artículo 9.2.j PPE-RGPD la mención a las sospechas de delito.

El supuesto de tratamiento necesario para que el responsable cumpla con el derecho laboral incluye expresamente lo que establezcan, además de la legislación, los convenios colectivos y se remite a lo establecido en las disposiciones sobre tratamientos específicos incluidas en el reglamento (art. 9.2.b que remite al art. 82 PPE-RGPD). También remiten a esta regulación el supuesto que permite el tratamiento de datos de salud (art. 9.2.h que remite al art. 81 PPE-RGPD) y los nuevos supuestos relativos al tratamiento necesario con fines de investigación histórica, estadística o científica (art. 9.2.i que remite al art. 83 PPE-RGPD) y al tratamiento de datos necesario para los servicios de archivos (art. 9.2.i bis que remite al art. 83bis PPE-RGPD). Se mantienen el resto de supuestos que ya se encontraban en la Directiva 95/46/CE sin variaciones[1684].

En la orientación del Consejo UE hay cambios respecto a esta regulación del texto parlamentario. Así, se puede mencionar que no se ha incluido el supuesto relativo al cumplimiento o ejecución del contrato. Respecto a los tratamientos de las administraciones se especifica que se deben realizar por motivos de interés público (art. 9.2.g) PCJ-RGPD). Se incluyen dos supuestos relativos a los fines sanitarios, ya que en este texto se ha suprimido la regulación específica relativa a este tipo de tratamientos, por lo que se ha tenido que suplir en el precepto (art. 9.h y hter PCJ-RGPD)[1685]. En este sentido, se ha introducido la posibilidad de que los Estados miembros legislen sobre los datos genéticos o de salud (art. 9.5 PCJ-RGPD) y que se puedan tratar todos los datos de categorías especiales, de acuerdo con la legislación de la UE o de los Estados miembros cuando esos datos se traten por o bajo la responsabilidad de profesionales sujetos a la obligación de secreto profesional (art. 9.4 PCJ-RGPD).

El Consejo UE ha eliminado el apartado relativo a los datos sobre sanciones y condenas porque se ha introducido un nuevo artículo con esta regulación. Aunque se refiere a menos datos (condenas y delitos penales o medidas de seguridad afines) también

[1684] Son los supuestos relativos al tratamiento para proteger el interés vital del interesado o de otra persona (art. 9.2.c PPE-RGPD), el tratamiento efectuado por una fundación, asociación o entidad sin ánimo de lucro con finalidad política, filosófica, religiosa o sindical, de acuerdo con las limitaciones establecidas (art. 9.2.d PPE-RGPD), el tratamiento que se refiera a datos que el interesado haya hecho manifiestamente públicos (art. 9.2.e PPE-RGPD), el tratamiento necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial (art. 9.2.f PPE-RGPD).

[1685] Se ha suprimido el artículo 81 PCE-RGPD relativo al tratamiento de datos personales relativos a la salud.

se establece la necesidad de supervisión de poderes públicos para poder tratarlos o que estuviera autorizado por la legislación (art. 9bis PCJ-RGPD).

También hay que señalar otra obligación novedosa y de asignación expresa al responsable que ya se ha comentado al examinar la responsabilidad del encargado del tratamiento. Si el responsable no pudiera identificar a una persona, no deberá tratar información adicional de la misma para identificarla, con el único fin de cumplir lo dispuesto en el reglamento (art. 10 PCE-RGPD). Se trata de evitar la perversión del cumplimiento de la normativa de protección de datos que puede originar que se traten datos personales con el solo propósito de cumplir con la misma, lo que sería contrario a su espíritu.

El Consejo UE cambia esta disposición, de forma que lo que indica es que si los fines para los cuales el responsable trataba los datos ya no requieren que se identifique al interesado, no deberá mantener ni obtener información adicional para identificar al mismo (art. 10.1 PCJ-RGPD). En estos casos dejarán de aplicarse los artículos relativos al ejercicio de derechos, a no ser que el interesado facilitara información que permita su identificación (art. 10.2 PCJ-RGPD).

Por último, el Parlamento incluyó, en la parte de los principios, una disposición que se titula "principios generales de los derechos de los interesados" y que enfatiza la importancia de estos derechos en la protección de datos[1686]. Así, se especifica que deben ser respetados por el responsable del tratamiento (art. 10bis.1 PPE-RGPD), cuyas solicitudes debe atender en un plazo razonable (art. 10bis.2 PPE-RGPD).

2.3.2. Las obligaciones derivadas de los derechos de los interesados

Los derechos de los interesados que se pueden encontrar en los tres textos son los de transparencia e información, acceso, portabilidad (según textos de la Comisión y el Consejo UE), supresión y derecho al olvido (este último solo en los textos de la Comisión

[1686] En este precepto se incluye el desglose de algunos de los derechos: "el suministro de información clara y fácilmente comprensible sobre el tratamiento, el derecho de acceso, rectificación y supresión, el derecho a la obtención de datos, el derecho a oponerse a la elaboración de perfiles, el derecho a presentar una reclamación ante la autoridad competente y a emprender acciones judiciales y el derecho a obtener una compensación por daños y perjuicios derivados de una operación ilícita." (art. 10bis.2 PPE-RGPD).

y el Consejo UE), oposición, limitación al tratamiento (solo en el del Consejo UE) y elaboración de perfiles (o decisión individual automatizada, según el Consejo UE).

Se incluye también la regulación que obviamente en la Directiva 95/46/CE no se había detallado sobre los procedimientos y mecanismos que debe cumplir el responsable del tratamiento, como el plazo para atender las solicitudes de ejercicio de los derechos que le dirijan los interesados (art. 12 PCE-RGPD)[1687].

En la regulación de los derechos, que se encuentra en el Capítulo III del reglamento, la primera Sección se dedica a la transparencia. Esta Sección se inicia con un precepto general que obliga al responsable, de forma expresa, a aplicar políticas transparentes sobre el tratamiento de los datos y el ejercicio de los derechos, así como a facilitar al interesado cualquier información relativa al tratamiento de forma inteligible, en particular cuando se destine a los menores (art. 11 PCE-RGPD). Este precepto se ha eliminado en la orientación general del Consejo UE, que lo ha traspasado a la parte del preámbulo (Considerando 46 PCJ-RGPD).

El deber de informar de la Directiva 95/46/CE, se ha reforzado, mediante el enunciado de este principio de transparencia, a través de la articulación del procedimiento a seguir, en caso de recibir una solicitud del interesado (art. 12 PCE-RGPD) y por la ampliación del contenido de información a proporcionar, en el momento de recogida de datos, especialmente en el texto del Parlamento (arts. 13bis y 14 PPE-RGPD)[1688]. El Parlamento ha incidido en la forma en la que debe proporcionarse esta información, que responde claramente al nuevo entorno digital y recoge las recomendaciones que el GA29

[1687] Este plazo, según el Parlamento será de cuarenta días y, según la Comisión y el Consejo UE, será de un mes.

[1688] Así, además de ampliarse el contenido de información mínima que debe proporcionarse en el momento de recogida al interesado, en el texto parlamentario, se ha previsto un paso previo en el que debe informarse de una serie de pormenores, mediante políticas de información normalizadas, en las que se presentarán estos pormenores con los iconos que se incluyen en anexo al Reglamento (art. 13bis PPE-RGPD). Con este mecanismo se pretende facilitar el cumplimiento de esta obligación y se aplican las indicaciones del GA29, que recomendaba en los entornos *online* la información por capas, para evitar complejas políticas, difíciles de asumir por un usuario medio. Ejemplo de aspectos de los que debe informar el responsable del tratamiento, que no se incluían en la Directiva 95/46/CE son: los datos del delegado de protección de datos (en su caso), información relativa a la seguridad del tratamiento, el plazo de conservación de los datos o los criterios para determinarlo, la intención de transferir los datos a países terceros u organizaciones internacionales, la existencia de elaboración de perfiles, la lógica utilizada en los tratamientos o información sobre el suministro de datos personales a las autoridades públicas durante el último período consecutivo de doce meses (art. 14 PPE-RGPD).

ha proporcionado al respecto[1689]. El Consejo UE ha preferido diferenciar, como se hacía en la Directiva 95/46/CE, entre la información que se proporciona en la recogida directa y la indirecta (arts. 14 y 14bis PCJ-RGPD)[1690].

Respecto a las novedades que incorpora el reglamento sobre las excepciones previstas a este deber de informar, el supuesto relativo al tratamiento de datos con fines de investigación histórica, estadística y científica, ya contemplado en la Directiva 95/46/CE para la recogida indirecta, ahora se amplía a la directa en el texto del Parlamento (art. 14.5.b PPE-RGPD)[1691]. Asimismo se incluye un nuevo supuesto de excepción a esta obligación relativo al tratamiento de datos por personas sujetas al secreto profesional (art. 14.5.dbis PPE-RGPD).

En lo referido a los derechos de acceso, rectificación, supresión y oposición, en la propuesta de la Comisión se ampliaron con nuevos derechos: el derecho al olvido y el derecho de portabilidad. Sin embargo, en el trámite parlamentario se eliminaron y se recondujeron a los derechos originarios. De forma paralela, el TJUE vehiculó la solicitud del derecho al olvido que el señor Costeja efectuó contra *Google* a la regulación establecida por la Directiva 95/46/CE, de forma que evitó la alusión a un nuevo derecho[1692]. Sin embargo, en la orientación general del Consejo UE se han mantenido estos derechos de olvido y portabilidad y se ha añadido el derecho a la limitación del tratamiento.

[1689] Especialmente en la Recomendación sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea, 5020/01/ES/Final WP 43, 17.5.2001, Grupo de trabajo Artículo 29 sobre la protección de datos y en el Dictamen 10/2004 sobre una mayor armonización de las disposiciones relativas a la información, 11987/04/ES WP 100, 25.11.2004, Grupo de trabajo Artículo 29 sobre la protección de datos.

[1690] El Consejo UE incluye, entre la información que se debe proporcionar la base jurídica del tratamiento (art. 14.1.b) y 14bis.1b PCJ-RGPD). También obliga a informar sobre los tratamientos ulteriores (art. 14.1ter y 14bis.3bis PCJ-RGPD). No obstante, no incluye algunos aspectos que establecía el texto del Parlamento ni tampoco la información previa sobre los pormenores. El GA29, en sus recomendaciones para los diálogos entre las instituciones, tras la adopción del Consejo de su orientación general, indicaba que debería informarse al interesado sobre los plazos de conservación, las garantías previstas en las transferencias internacionales y las medidas de seguridad adoptadas. *Annex to letters in view of the trilogue: Core topics in view of the trilogue, 17.6.2015, Article 29 Working Party,* pág. 11.

[1691] No obstante, la redacción es algo confusa, ya que se une esta excepción a la establecida para los datos no recogido directamente del interesado y cuya información resulte imposible o implique un esfuerzo desproporcionado. En la orientación del Consejo UE sólo se incluyen excepciones en la recogida indirecta. Sin embargo, no se alude la excepción al deber de informar cuando se traten datos con estos fines de investigación histórica, estadística o científica pero porque se incluye, para la recogida indirecta, en el artículo 83 PCJ-RGPD y se añade la finalidad de archivo en interés público.

[1692] Ver Capítulo VIII y Sentencia del TJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2014:317.

En el derecho de acceso, se incluye, tanto el derecho a que el responsable del tratamiento indique al interesado si realiza un tratamiento o no de sus datos y le proporcione información acerca de una serie de aspectos que describen el tratamiento, como el derecho a obtener una copia de estos datos (art. 15.1 y .2 PCE-RGPD). De esta forma, gracias al derecho de acceso, el interesado puede conocer y verificar la licitud del tratamiento (Considerando 51 PCE-RGPD).

La resolución del Parlamento, al eliminar el derecho a la portabilidad, lo que hizo fue encauzar este derecho a la portabilidad en este derecho de obtención de una copia de los datos. De esta forma, el responsable, si se lo solicita el interesado, si fuera técnicamente viable y materialmente posible, deberá proporcionarle los datos personales a otro responsable (15.2bis PPE-RGPD). No obstante, el precepto queda debilitado, al introducir la posibilidad de valorar si esta portabilidad es viable o posible.

El Consejo UE mantuvo el derecho a la portabilidad, en un artículo separado, para los casos en los que el tratamiento se realizara en virtud de la base jurídica del consentimiento o la ejecución de un contrato o medidas precontractuales (art. 18.2 PCJ-RGPD). Sin embargo, introdujo excepciones a su cumplimiento, como en caso de que el tratamiento sea necesario para una misión de interés público o inherente al ejercicio del poder público, o si se pudieran vulnerar derechos de propiedad intelectual (art. 18.2bis y .2bis bis PCJ-RGPD).

Asimismo, el Consejo UE también incluyó la regulación de la obtención de una copia de los datos en el derecho de acceso (art. 15.1ter y 2bis PCJ-RGPD). En esta disposición se establece como excepciones a la entrega de la copia: cuando no sea posible facilitarla sin revelar datos de otros interesados o datos confidenciales o cuando se vulneren los derechos de propiedad intelectual. El GA29 ha indicado que el derecho de acceso es esencial en la regulación y, especialmente, la primera excepción reduciría este derecho sin una adecuada justificación[1693].

[1693] *Annex to letters in view of the trilogue: Core topics in view of the trilogue, 17.6.2015, Article 29 Working Party,* pág. 12.

El derecho de rectificación, que ha permanecido sin cambios relevantes en los tres textos, posibilita al interesado solicitar la corrección de los datos cuando resulten inexactos y también que los pueda completar (art. 16 PCE-RGPD).

En lo que se refiere al derecho a la supresión de datos personales, además de introducir en el texto de la Comisión y del Consejo UE la denominación de derecho al olvido, se ha ampliado considerablemente su regulación, en comparación con la de la Directiva 95/46/CE[1694]. De esta forma, se incorpora una compleja arquitectura jurídica, en la que se establecen una serie de supuestos en los que el interesado tendrá el derecho a que el responsable suprima sus datos, pero que estarán excepcionados por otros supuestos que permitirán la conservación de los datos o la limitación del tratamiento.

El texto de la Comisión establece el derecho del interesado a que el responsable suprima sus datos si concurren los supuestos establecidos (art. 17.1 PCE-RGPD)[1695]. La adaptación al entorno *online* se refleja especialmente en una obligación adicional del responsable que, si debiera suprimir los datos, de acuerdo con el artículo 17.1 PCE-RGPD, y si los hubiera hecho públicos, deberá tomar medidas para que los terceros que puedan enlazar a estos datos o realizar copia de los mismos, también los eliminen (art. 17.2 PCE-RGPD). Así, quien publique datos en un sitio web, deberá adoptar las medidas necesarias para evitar que los terceros eliminen los enlaces o las copias de los datos sobre los que el interesado pueda haber solicitado la supresión. Estos terceros serían claramente los buscadores pero pueden ser otros titulares de sitios web. La Comisión para evitar el efecto multiplicador de Internet pretendía obligar al responsable que publicaba los datos en un sitio web a que los eliminara y a que hiciera lo posible por parar la difusión, por ejemplo, evitando la indexación por parte de los buscadores[1696].

[1694] Hay que tener en cuenta que en el artículo 12 Directiva 95/46/CE se incluye la regulación del derecho de acceso y dentro de éste se contempla la rectificación, supresión o el bloqueo de datos cuyo tratamiento no se ajuste a la directiva.

[1695] Estos supuestos que establece la propuesta de la Comisión son: cuando los datos ya no sean necesarios para los fines para los que se recogieron o trataron; cuando el interesado retire su consentimiento de acuerdo con el artículo 6.1.a PCE-RGPD o haya expirado el plazo de conservación autorizado y no exista otro fundamento jurídico para el tratamiento; cuando el interesado se oponga al tratamiento ex artículo 19 PCE-RGPD; si el tratamiento no es conforme con el reglamento por otros motivos (art. 17.1 PCE-RGPD).

[1696] Como indicaba TRONCOSO REIGADA, la Comisión construyó el derecho al olvido sobre las obligaciones del responsable principal, del titular del sitio web que publica los datos y rechazó, por tanto, hacer responsable al buscador que enlazaba a la información. A. TRONCOSO REIGADA, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *Revista Española de Derecho Europeo*, *op. cit.*, págs. 74 a 75.

La resolución del Parlamento parece reforzar el papel del tercero, ya que indica, de entrada que "el interesado tendrá derecho a que el responsable del tratamiento suprima los datos personales que le conciernen y se abstenga de darles más difusión y, en relación con terceros, a que estos supriman todos los enlaces a los datos personales, copias o reproducciones de los mismos" en los supuestos que especifica (art. 17.1 PPE-RGPD)[1697].

Respecto a la obligación adicional señalada en la propuesta de la Comisión, el Parlamento lo modifica, de manera que el responsable que haya hecho públicos los datos, sin ninguna base jurídica válida de las establecidas en el artículo 6.1 PPE-RGPD, deberá adoptar las medidas razonables para que los datos sean suprimidos por el tercero y, cuando fuera posible, informará a los interesados de las medidas adoptadas por este tercero, y ello sin perjuicio del derecho del interesado a obtener una compensación (art. 17.2 PPE-RGPD).

El Consejo UE, en la línea de la propuesta de la Comisión, establece el derecho del interesado a que el responsable suprima los datos en los supuestos indicados sin nombrar al tercero (art. 17.1 y .1bis PCJ-RGPD)[1698]. Respecto a la obligación añadida del responsable cuando haya hecho públicos los datos, deberá adoptar las medidas razonables para informar a los responsables que traten los datos de que el interesado les solicita la supresión de cualquier enlace a esos datos o cualquier copia o réplica de los mismos (art. 17.2bis PCJ-RGPD). Por tanto, respecto a esta obligación, el Consejo UE, a diferencia de la Comisión y del Parlamento, no menciona al tercero, sino que se refiere a otros responsables. Entiendo que ello se debe a que, cuando el Consejo UE adoptó su orientación general, el TJUE ya se había pronunciado sobre el asunto *Google*[1699]. El buscador encajaba claramente en el papel de tercero al que apuntaban los textos de la

[1697] Estos supuestos, en el texto del Parlamento, son los mismos que en el texto de la Comisión pero se añade cuando un tribunal o una autoridad con sede en la UE ha dictaminado que han de suprimirse los datos y, en lugar del supuesto referido a que el tratamiento no fuera conforme con el reglamento se cambia por cuando los datos hayan sido tratados ilícitamente (art. 17.1 PPE-RGPD).

[1698] El Consejo UE incluye los siguientes supuestos: cuando los datos ya no sean necesarios para los fines para los que se recogieron o trataron; cuando el interesado retire el consentimiento en el que se fundamenta el tratamiento de acuerdo con el artículo 6.1.a) PCJ-RGPD o con el artículo 9.2.a) PCJ-RGPD y no exista otro fundamento jurídico para el tratamiento; cuando el interesado se oponga al tratamiento ex artículo 19 PCJ-RGPD; si los datos han sido tratados ilícitamente, si los datos deben suprimirse para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable y si los datos se han obtenido con relación a la oferta de servicios de la sociedad de la información previstos en el artículo 8.1 PCJ-RGPD (art. 17.1.e) y 17.1bis PCJ-RGPD).

[1699] Sentencia del TJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2014:317.

Comisión y el Parlamento. Antes de esta sentencia no estaba claro si se podía considerar a los buscadores responsables del tratamiento respecto a los datos personales que figuraban en los enlaces de los resultados de las búsquedas. Sin embargo, el TJUE consideró que *Google* era responsable del tratamiento y, como tal, debía atender la solicitud del interesado. En consecuencia, el Consejo UE entiende que estamos ante otro responsable y, por eso lo califica como tal en el precepto.

Como se ha mencionado, respecto a la obligación de supresión, se establecen unas excepciones que permitirán al responsable o al tercero (en el caso del texto parlamentario) no tener que suprimir los datos, ya sea porque es necesario que los conserven, o porque es posible limitar el tratamiento, lo que equivaldría al bloqueo que recogía el artículo 12.b) Directiva 95/46/CE[1700]. El Consejo UE, en su orientación, ha separado esta regulación del bloqueo en un derecho independiente que ha denominado "derecho a la limitación del tratamiento" (art. 17bis PCJ-RGPD).

Se establece, como obligación de asignación expresa al responsable, la comunicación a los destinatarios a los que haya transferido los datos de cualquier rectificación o supresión que lleve a cabo de los datos y el Parlamento añade que el responsable, además, informará al interesado sobre estos destinatarios si este lo solicita (art. 13 PPE-RGPD)[1701].

[1700] Así, se permitiría la conservación de los datos, según el texto del Parlamento: para el ejercicio del derecho a la libertad de expresión, de acuerdo con lo previsto en el artículo 80 PPE-RGPD; por motivos de interés público en el ámbito de la salud pública, de acuerdo con el artículo 81 PPE-RGPD; con fines de investigación histórica, estadística y científica de conformidad con el artículo 83 PPE-RGPD; para el cumplimiento de una obligación de conservación prevista en la legislación de la UE o de un Estado miembro (art. 17.3 PPE-RGPD). Los supuestos en los que se procedería al bloqueo serían cuando el interesado impugne la exactitud de los datos, durante el plazo que permita al responsable verificarlo; cuando el responsable necesite los datos a efectos probatorios; cuando el tratamiento sea ilícito y sea el interesado quien se oponga a su supresión; cuando un tribunal o una autoridad con sede en la UE haya dictaminado que ha de limitarse el tratamiento; cuando el interesado solicite la transmisión a otro sistema automatizado conforme a la portabilidad establecida en el artículo 15.2bis PPE-RGPD; cuando el tipo de tecnología de conservación no permita la supresión siempre que ésta se hubiera puesto en práctica antes de la entrada en vigor del PPE-RGPD (art. 17.4 PPE-RGPD). Sin embargo, pese a que este artículo 17.3 PPE-RGPD, en uno de estos supuestos (el apartado e) remite a los casos en los que se permitirá el bloqueo (que se desglosan en el art. 17.4 PPE-RGPD), cuando se revisan estos casos, sólo se alude al responsable del tratamiento como el sujeto que puede proceder al bloqueo y no se menciona al tercero.

[1701] El Consejo UE mueve este precepto al artículo 17ter PCJ-RGPD y también incluye la notificación respecto al derecho de restricción del tratamiento. A diferencia del Parlamento, el Consejo UE no dispone que el responsable deba informar si el interesado se lo solicita.

Estas previsiones que tienen como objetivo que el responsable se dirija a otros sujetos para velar porque el tratamiento de datos que realizan estos respete la voluntad del interesado, confirman el papel del responsable de garante del derecho a la protección de datos de los afectados. Es el responsable quien está en posición de asegurar esta protección y, por ello se quiere extender esta capacidad de protección al máximo.

Otra obligación de asignación expresa al responsable es que dejará de usar o tratar los datos personales, cuando el interesado ejerza su derecho a oponerse al tratamiento, en los casos establecidos en el artículo 19 PCE-RGPD. La Comisión y el Parlamento dispusieron este derecho de oposición para tratamientos originados por las bases jurídicas contenidas en el artículo 6.1 apartados d), e) y f), es decir, para proteger intereses vitales del interesado, por motivos de interés público, de ejercicio del poder público o por los interese legítimos del responsable del tratamiento. En cambio el Consejo UE, sólo ha contemplado el derecho de oposición respecto a los apartados e) y f) (art. 19.1 PCJ-RGPD)[1702].

Por tanto, en el texto del Parlamento se incorpora el supuesto de protección de intereses vitales que no se hallaba en el artículo 14 Directiva 95/46/CE. Asimismo se refuerza este derecho de oposición, ya que en la directiva el interesado debía ejercerlo, por razones legítimas propias de su situación particular y justificarlo. En la resolución parlamentaria, cuando el tratamiento se realice en virtud de intereses legítimos del responsable, el interesado podrá oponerse sin necesidad de justificación (art. 19.2 PPE-RGPD). En caso de que se trate de los otros dos supuestos relativos al tratamiento para protección de intereses vitales y el interés público, lo que se plantea es que el interesado tendrá derecho de oposición, excepto si el responsable acredita motivos imperiosos y legítimos para el tratamiento que prevalezcan sobre los intereses y libertades fundamentales del interesado (art. 19.1 PPE-RGPD).

El Parlamento establece también un derecho de oposición respecto a la elaboración de perfiles (art. 20.1 PPE-RGPD), obligación de asignación implícita al responsable. No incluye, como en la Directiva 95/46/CE, la regulación de la oposición en

[1702] El GA29 ha manifestado que debería incrementarse el nivel de protección respecto al existente con la Directiva 95/46/CE y, en consecuencia, extender la posibilidad de ejercer el derecho de oposición a más supuestos de los ya establecidos en la misma. *Annex to letters in view of the trilogue: Core topics in view of the trilogue, 17.6.2015, Article 29 Working Party*, pág. 13.

caso de tratamiento de datos destinado a la prospección (art. 14.b) Directiva 95/46/CE) porque este fin, el Parlamento entiende que cabe en la base jurídica relativa al interés legítimo (Considerando 39ter PPE-RGPD).

En cambio, el Consejo UE no establece este derecho de oposición para lo que denomina decisiones individuales automatizadas y que se corresponden a la elaboración de perfiles en los textos de la Comisión y el Parlamento (art. 20.1 PCJ-RGPD). Sin embargo, el Consejo UE, al igual que la Comisión, sí establece la oposición en el caso de los tratamientos de datos con fines de marketing directo y también para los tratamientos con fines históricos, estadísticos o científicos (art. 19.2 PCJ-RGPD).

También se destaca la importancia que se ha otorgado a la elaboración de perfiles que dé lugar a medidas que produzcan efectos jurídicos que atañan al interesado o afecten a sus intereses, derechos o libertades, lo que en el artículo 15 Directiva/95/46/CE se conocía como las decisiones individuales automatizadas, denominación que, como se ha visto, ha decidido mantener el Consejo UE.

Si bien se ha preservado la regulación básica establecida en la Directiva/95/46/CE, el Parlamento hace alusión específica a la prohibición de discriminación y de uso de categorías especiales de datos (art. 20.3 PPE-RGPD)[1703]. Otro aspecto en el que se incide en este derecho, además del informativo, es en el de garantizar que exista una evaluación humana y la explicación de la decisión adoptada (art. 20.5 PPE-RGPD). Además, se puede ver la tendencia al papel proactivo del responsable que debe aplicar medidas de protección para evitar la discriminación en este tipo de tratamientos, lo que se configura como una obligación de asignación expresa (art. 20.3 PPE-RGPD). Estas medidas adquieren una gran relevancia ante el desarrollo tecnológico de los mecanismos que posibilitan estas evaluaciones automáticas, como el uso de algoritmos.

[1703] Además, el Parlamento europeo introdujo una definición de "elaboración de perfiles" como "toda forma de tratamiento automatizado de datos personales destinado a evaluar determinados aspectos personales propios de una persona física o a analizar o predecir en particular su rendimiento profesional, su situación económica, su localización, su estado de salud, sus preferencias personales, su fiabilidad o su comportamiento" (art. 4.3bis PPE-RGPD). Por otro lado, el Considerando 58bis PPE-RGPD establecía una presunción de que la elaboración de perfiles en la que se utilicen seudónimos no afecta de modo significativo a los intereses, derechos o libertades del interesado. Ahora bien, matiza el propio considerando que si el responsable del tratamiento puede atribuir los datos seudónimos a un interesado concreto, ya sea a partir de una sola fuente de datos seudónimos, o a partir de la suma de datos seudónimos de diversas fuentes, no deberán considerarse estos datos seudónimos.

El GA29, no obstante, ha alertado que la orientación del Consejo UE no es suficientemente clara ni incluye suficientes medidas de protección frente a la elaboración de perfiles[1704]. Así el Consejo UE no ha previsto la adopción de las medidas para evitar la discriminación ni ha establecido la prohibición de que las decisiones se adopten, única o predominantemente, en virtud de un tratamiento automatizado, medidas que preveía el Parlamento.

En el texto parlamentario se aprecia una mayor conexión entre los derechos. Así, entre el contenido de la información que debía proporcionarse en virtud del artículo 14 PPE-RGPD, se debía indicar la existencia de tratamientos de datos para la elaboración de perfiles y también la lógica utilizada en los tratamientos automatizados (art. 14.1.gbis y gter PPE-RGPD). También se observa el paralelismo entre la información que se debe proporcionar al interesado y la que se debe proporcionar en virtud del derecho de acceso de los datos.

Por último, hay que hacer mención de las limitaciones previstas a estos derechos, que pueden realizarse mediante el derecho de la UE o de un Estado miembro, en virtud de los objetivos que se señalan, como la seguridad pública o la protección de los derechos y libertades de otras personas (art. 21 PCE-RGPD)[1705]. El GA29 alerta de la inclusión por parte del Consejo UE de nuevos supuestos demasiado amplios, como los objetivos importantes de interés público general de la UE o de un Estado miembro, o la ejecución de demandas civiles[1706].

[1704] *Annex to letters in view of the trilogue: Core topics in view of the trilogue, 17.6.2015, Article 29 Working Party*, pág. 14.
[1705] Respecto a estos límites establecidos por el artículo 21 PCE-RGPD y, de manera amplia, sobre los límites al derecho a la protección de datos que se pueden encontrar en el texto del reglamento, así como los requisitos establecidos para estos límites en la Carta UE, en el CEDH y en la jurisprudencia del TC, ver: A. TRONCOSO REIGADA, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *Revista Española de Derecho Europeo*, *op. cit.*, págs. 86 a 128.
[1706] *Annex to letters in view of the trilogue: Core topics in view of the trilogue, 17.6.2015, Article 29 Working Party*, pág. 13.

2.3.3. Las obligaciones derivadas de la regulación de las transferencias internacionales de datos

La Comisión y el Parlamento incluyeron en sus textos un principio general relativo a las transferencias de datos personales a un tercer país o a una organización internacional, que establece el responsable y el encargado solo las podrán realizar si cumplen las condiciones establecidas en el capítulo V del reglamento, en particular en lo tocante a las transferencias ulteriores (art. 40 PCE-RGPD). Este principio fue suprimido por el Consejo UE.

Como primeras diferencias respecto a la Directiva 95/46/CE, se pueden indicar la posibilidad de que la transferencia se dirija a organizaciones internacionales y que los sujetos que podrán transferir datos ya no son solo los responsables del tratamiento, sino que también podrán ser encargados del tratamiento. En esta regulación se incorporan los instrumentos creados por las autoridades de control en el seno del GA29 y el reflejo del conflicto ya apuntado que existe con los EEUU.

Las posibilidades establecidas para que se permitan las transferencias a países terceros o a organizaciones internacionales se deben escoger de acuerdo con un orden de preferencia: la primera opción será que la Comisión Europea haya adoptado una decisión favorable a la adecuación del nivel de protección proporcionado por el país, un territorio o un sector del tratamiento de datos en ese país o la organización internacional (art. 41 PCE-RGPD); si no hay decisión de la Comisión, la segunda posibilidad es que el responsable o el encargado del tratamiento ofrezcan las garantías apropiadas mediante un instrumento jurídicamente vinculante (art. 42 PCE-RGPD) y, por último, si no se puede optar por ninguna de las dos anteriores, quedará que el supuesto se encaje en alguna de las excepciones que permitirán realizar la transferencia (art. 44 PCE-RGPD).

Las garantías que pueden ofrecer el responsable o el encargado para realizar las transferencias, en la segunda opción señalada, las podemos dividir, entre las que no requieren de autorización de la autoridad de control y las que sí. De acuerdo con la resolución del Parlamento, las siguientes no requieren autorización: las normas corporativas vinculantes o *Binding Corporate Rules*, el “Sello Europeo de Protección de

Datos" y las cláusulas tipo de protección de datos adoptadas por una autoridad de control si la Comisión declara su validez general (art. 42.2 PPE-RGPD). Como garantía que requiere de autorización de la autoridad de control se establecieron las cláusulas contractuales entre responsable o encargado y destinatario.

El Consejo UE, en su orientación general, añadió a las garantías que no requieren de autorización, establecidas por el Parlamento, las siguientes: un instrumento jurídicamente vinculante y ejecutivo entre autoridades u organismos públicos, cláusulas tipo adoptadas por la Comisión, un código de conducta o un mecanismo de certificación aprobados de acuerdo con el reglamento[1707] (art. 42.2 PCJ-RGPD). Respecto a las que requerían de autorización modificó la de las cláusulas contractuales, para precisar que podrían establecerse entre responsable o encargado o destinatario en el tercer país u organización internacional, y se añadió otra garantía que eran las disposiciones que se incluyan en acuerdos administrativos entre autoridades u organismos públicos (art. 42.2bis PCJ-RGPD).

Las diferencias más importantes respecto a los mecanismos vigentes son que no será necesario solicitar autorización en los supuestos señalados y que se pueden utilizar códigos de conducta y mecanismos de certificación, como garantía.

Se incluye en los textos la regulación detallada de la aprobación de las normas corporativas vinculantes que se definen como:

> "Las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro de la Unión para las transferencias o un conjunto de transferencias de datos personales a un responsable o encargado del tratamiento en uno o más países terceros, dentro de un grupo de empresas" (art. 4.17 PCE-RGPD).

El Consejo UE añadió a esta definición "o grupos de sociedades que participen en una actividad económica conjunta", por lo que abriría aún más las posibilidades de utilización de estas normas.

[1707] Por lo que se suprimiría la garantía del "Sello Europeo de Protección de Datos" que no se incorporó en el texto del Consejo UE.

Entre los aspectos contemplados en esta regulación, dentro del contenido mínimo que debe constar en las normas, se exige la aceptación del responsable o de encargado europeos de la responsabilidad, por cualquier violación de las normas corporativas, por parte de cualquier miembro del grupo que no esté establecido en la UE (art. 43.2.f) PCE-RGPD). El responsable o el encargado sólo podrán ser exonerados si prueban que el acto que originó el daño no es imputable a dicho miembro. No obstante, si bien la Comisión y el Consejo UE han establecido esta responsabilidad para el responsable o el encargado, el Parlamento únicamente ha estimado que el responsable europeo debía ser el responsable (art. 43.2.f PPE-RGPD). Por tanto, se puede ver la dificultad en la articulación de las responsabilidades entre responsable y encargado, en un sistema en el que sólo había un responsable, ahora es difícil valorar hasta dónde debe llegar la responsabilidad de uno o del otro.

Respecto a las excepciones se mantienen las incluidas en la Directiva 95/46/CE aunque se han introducido algunas precisiones. El consentimiento del interesado será explícito y exigirá que se informe de los riesgos que entraña la transferencia debido a la ausencia de decisión de adecuación y de garantías apropiadas (art. 44.1.a PCE-RGPD).

La excepción que permite realizar transferencias, cuando sea necesario por motivos importantes de interés público, se completa mediante la exigencia de que este interés público esté reconocido, en el derecho de la UE o del Estado miembro al que esté sujeto el responsable del tratamiento (art. 44.5 PCE-RGPD). La transferencia, en este supuesto, según el Parlamento, sólo podrá realizarse de forma ocasional (Considerando 87 PPE-RGPD). Respecto al sector público también se indica que no podrá utilizar las excepciones relativas a la ejecución del contrato o medidas precontractuales y a la ejecución de contrato en interés del interesado (art. 44.4 PCE-RGPD)[1708].

La Comisión había incluido entre las excepciones la posibilidad de transferir datos en virtud del interés legítimo del responsable o del encargado, en transferencias no frecuentes ni a gran escala y siempre que se adoptaran garantías apropiadas (art. 44.1.h) PCE-RGPD). El Parlamento lo suprimió pero el Consejo lo ha vuelto a introducir en su orientación general, aunque ha corregido que el interés legítimo debe ser del responsable

[1708] También se añadía el supuesto relativo al interés legítimo que se comenta a continuación.

(art. 44.1.h) PCJ-RGPD). No obstante, en la parte del preámbulo, se ha mantenido la alusión al interés legítimo del responsable o del encargado, por lo que no queda claro si se entiende que el encargado puede realizar la transferencia en virtud de un interés legítimo propio (Considerando 88 PCJ-RGPD). A esto se añade que en el precepto se establece que el responsable o el encargado (se entiende que depende de quién realice la transferencia) realizarán la evaluación de las circunstancias que rodean el tratamiento, para ver las garantías que deben adoptarse ¿Significa que el encargado podrá realizar una transferencia, en virtud de una base jurídica que determinará él mismo? ¿No supondría que el encargado determinaría los fines del tratamiento y, por tanto, debería calificarse como responsable? Al otorgar un papel tan relevante al encargado, en el reglamento, se corre el riesgo de no dejar claro quién debe tener el control sobre el tratamiento.

El GA29 ha considerado que esta excepción relativa al interés legítimo es demasiado amplia y ha recomendado que, si se mantiene se utilice sólo de forma puntual y se informe a los afectados[1709].

Sin duda, la tensión existente con los EEUU se percibe en las modificaciones realizadas especialmente en el proceso de tramitación parlamentaria del reglamento. Ya se comentó la introducción del artículo 43bis PPE-RGPD pero son numerosas las alusiones y restricciones incorporadas en la regulación de las transferencias dirigidas a intentar proteger los datos objeto de estas transferencias de posibles accesos por parte de autoridades extranjeras[1710]. Ejemplo de la compleja situación existente es que el Parlamento incluyó en el preámbulo del reglamento que, si los responsables o encargados

[1709] *Annex to letters in view of the trilogue: Core topics in view of the trilogue, 17.6.2015, Article 29 Working Party*, pág. 19.

[1710] Así, en lo referido a las decisiones de adecuación, se prevé no sólo que la Comisión pueda declarar la adecuación, sino que pueda realizar una declaración negativa de adecuación o puede declarar que se ha dejado de garantizar el nivel adecuado (art. 41.5 PCE-RGPD). Estas últimas declaraciones negativas podrán deberse a que la legislación del tercer país no garantice derechos eficaces y exigibles, como el derecho a recurso de los interesados. El Parlamento incluyó en la parte del preámbulo que si esta legislación del tercer país permite un acceso extraterritorial a los datos tratados en la UE, sin que la ley de la UE o de un Estado miembro lo permita, también se considerará indicativo de falta de adecuación (Considerando 82 PPE-RGPD). Clara alusión, por tanto, a lo reclamado actualmente por la Comisión en la negociación de la Decisión *Safe Harbour*. Además, entre los criterios que tendrá en cuenta para adoptar la decisión de adecuación, la Comisión deberá examinar la legislación del país tercero, tanto general como sectorial, las normas profesionales, las medidas de seguridad, y también, y aquí está la novedad, lo que se refiera a la seguridad, el derecho penal y la aplicación de la legislación, los precedentes jurisprudenciales y los derechos efectivos y exigibles, como los mencionados de recurso administrativo y judicial (art. 41.2.a PPE-RGPD). Asimismo, la Comisión deberá realizar un seguimiento continuo de las novedades que se produzcan en los países y organizaciones que pudieran afectar a la decisión de adecuación (art. 41.4bis PPE-RGPD).

se enfrentan a requisitos contradictorios entre lo que dice la normativa de la UE y lo que dice la del tercer país, podrán acudir a la Comisión para que resuelva el conflicto (Considerando 90 PPE-RGPD).

2.4. Los derechos o facultades

En primer lugar, hay que destacar un derecho del responsable del tratamiento establecido de forma expresa en la resolución del Parlamento. El responsable tiene derecho a transmitir datos personales dentro de la UE en el seno del grupo de empresas al que pertenezca para fines administrativos, cuando se establezcan disposiciones internas o códigos de conducta (art. 22.3bis PPE-RGPD). Esta disposición permite flexibilizar las comunicaciones de datos en el seno de grupos de empresas europeas si el objetivo es la gestión administrativa, lo que permitiría la centralización de esta gestión, algo muy habitual[1711]. De esta forma, se incentivaría la autorregulación, que permitiría realizar estas transmisiones, con una especie de normas corporativas vinculantes para transferencias intracomunitarias en el seno de un grupo de empresas. No obstante, el Consejo UE no ha incluido este precepto en su orientación general.

Sin realizar un examen exhaustivo de las posibles facultades que se derivan de las obligaciones establecidas en los tres textos, se puede indicar, en virtud de la resolución del Parlamento que, el responsable podrá tratar datos si puede acogerse a alguna base jurídica incluida en el principio de licitud (art. 6 PPE-RGPD) y en los preceptos relativos a categorías especiales de datos (art. 9 PPE-RGPD), tratamientos relativos a menores (art. 8 PPE-RGPD) o las disposiciones especiales (arts. 80 ss. PPE-RGPD).

El responsable podrá acogerse a la posibilidad de no recoger información adicional para tratar datos del interesado (art. 10 PPE-RGPD) y a las excepciones que se incluyen en los derechos de los interesados, así como a las limitaciones que puedan establecer los Estados miembros (arts. 11ss PPE-RGPD).

[1711] Este artículo establece que esto será posible "cuando su tratamiento sea necesario para fines administrativos internos legítimos entre sectores de actividades conexos del grupo de empresas y se garantice un nivel adecuado de protección de datos, junto con los intereses de los interesados, mediante disposiciones internas de protección de datos o códigos de conducta." (art. 22.3bis PPE-RGPD)

En su relación con el encargado del tratamiento el responsable dictará las instrucciones que éste debe seguir en el tratamiento de los datos y podrá autorizarle para que contrate otro encargado del tratamiento. También podrá recurrir al encargado para cumplir las obligaciones de los artículos 30 a 34 PPE-RGPD (en materia de seguridad, notificación de violaciones de datos, evaluaciones de impacto y consultas previas) y para poder atender el ejercicio de derechos por parte de los interesados. Asimismo, el responsable recibirá los resultados del tratamiento del encargado al término de éste y la información necesaria para demostrar el cumplimiento de las obligaciones relativas al encargo del tratamiento, además de poder realizar inspecciones *in situ* a éste (art. 26.2 PPE-RGPD).

El responsable no deberá comunicar la violación de datos al interesado si ha implementado medidas de protección tecnológica apropiadas a los datos afectados por la violación (art. 32.2 PPE-RGPD). Asimismo, si es una autoridad u organismo público y el tratamiento se efectúa, en cumplimiento de una obligación legal, no deberá realizar la evaluación de impacto prevista en los apartados 1 a 4 del artículo 33 PPE-RGPD, a no ser que los Estados miembros establezcan lo contrario (art. 33.5 PPE-RGPD).

Si está en un grupo de empresas podrán nombrar un delegado principal de protección de datos responsable (art. 35.2 PPE-RGPD) y si es una autoridad u organismo público podrá designar un delegado de protección de datos para varias de sus entidades. Cuando no sea obligatorio nombrar a un delegado de protección de datos podrá hacerlo, así como las asociaciones y organismos que le representen (art. 35.4 PPE-RGPD).

Las asociaciones u organismos que representen al responsable podrán someter sus códigos de conducta al dictamen de la autoridad de control o a la Comisión (si el ámbito se refiere a más de un Estado miembro) (art. 38.2 y 3 PPE-RGPD)[1712]. Además el responsable también podrá solicitar a cualquier autoridad de control que certifique que el tratamiento de datos que realiza se efectúa de conformidad con el reglamento (art. 39.1 PPE-RGPD). También tendrá derecho a obtener de la autoridad de control información general sobre sus responsabilidades y obligaciones (art. 52.2bis PPE-RGPD).

[1712] Respecto a estos mecanismos hay que resaltar que el Consejo UE ha puesto especial enfásis en la utilización de la autorregulación, por lo que ha incluido en algunos preceptos la posibilidad de acudir a estos instrumentos para tenerlos en cuenta, a la hora de valorar el cumplimiento, por parte del responsable (arts. 22, 23, 30, 33 PCJ-RGPD).

El responsable podrá realizar una transferencia internacional si es a un país u organización internacional sobre el que se haya declarado el nivel adecuado de protección (art. 41 PPE-RGPD) o si ofrece garantías adecuadas (art. 42 PPE-RGPD) o si se acoge a alguna de las excepciones previstas (art. 44 PPE-RGPD).

2.5. Garantías en el marco de la reforma

Ya hemos visto como se ha ampliado el abanico de derechos que tienen los interesados para acudir ante el responsable. Asimismo se ha resaltado la adopción de un sistema de autorresponsabilidad en el cumplimiento de las obligaciones del responsable. Todo ello se materializa en el diseño por el reglamento de una potente estrategia preventiva que quiere evitar las vulneraciones de los derechos antes de que se produzcan o, al menos, asegurar una rápida restitución de la situación vulneradora[1713]. Sin embargo, esta estrategia no supone el abandono de las garantías represivas y reparadoras.

El reglamento dedica su capítulo VIII, a imagen y semejanza del capítulo III de la Directiva 95/46/CE, a los recursos, responsabilidad y sanciones. Sin embargo, es evidente que la regulación se modifica, de forma que se desarrolla y detalla, con el fin de aportar la concreción que es precisa en una norma de directa aplicación como es el reglamento europeo.

Las autoridades de control adquieren, en este nuevo marco normativo, una clara relevancia, como garantía de los derechos de los afectados. Asimismo, con el fin de disminuir la carga administrativa a los responsables y encargados, uno de los objetivos, al adoptarse el reglamento, era dotarlo de un sistema de ventanilla única. Este sistema perseguía que un responsable o un encargado que estuviera establecido en varios Estados miembros, sólo tuviera que relacionarse con una única autoridad de control en caso de cualquier actuación derivada del cumplimiento del reglamento.

La consecución de este sistema de ventanilla única ha sido uno de los aspectos más complejos contemplados por el reglamento y, sin duda, es uno de los mayores retos

[1713] A. RALLO LOMBARTE, "Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma", *UNED, Revista de derecho político, op. cit.*, pág. 50.

al que se enfrentan las autoridades de control. No es objeto del presente trabajo abordar los detalles de este modelo. Sin embargo, es interesante aproximarnos al criterio para determinar la autoridad principal competente, donde se asiste de nuevo a la utilización del concepto de responsable como factor clave.

2.5.1. Las autoridades de control

En el reglamento se confirma la relevancia de las autoridades de control, garantía específica del derecho a la protección de datos, reconocida en la propia Carta UE, como ya vimos[1714]. La independencia de estas autoridades se proclama en los textos como carácter principal de estas entidades, de forma que se lleva a la rúbrica del Capítulo VI del reglamento, dedicado a las "Autoridades de control independientes" y, en concreto, a su Sección 1 que se titula "Independencia".

La autoridad de control actuará con total independencia en el ejercicio de las funciones y los poderes que se le otorgan en el reglamento y sus miembros, cuando ejerzan sus funciones, no solicitarán ni aceptarán instrucciones de nadie (art. 47 PCE-RGPD). En el reglamento, se articulan los mecanismos que posibilitarán que esta independencia sea efectiva, mediante una adecuada asignación de recursos propios y el refuerzo de las funciones y poderes de estas autoridades.

El GA29 da paso al Consejo Europeo de Protección de Datos que tendrá un papel más relevante y decisorio. Este órgano seguirá compuesto por los directores de las autoridades de control europeas y es el que se pretende que asegure, mediante el mecanismo de coherencia, la actuación homogénea de las autoridades.

La Comisión Europea también ha adoptado un papel más preponderante con la posibilidad de adoptar actos de ejecución o delegados, para desarrollar el reglamento. Sin embargo, esta capacidad ha sido criticada por el GA29, como una interferencia, precisamente, a la independencia de las autoridades de control[1715] y se ha recortado progresivamente en los textos del Parlamento y del Consejo UE.

[1714] Ver Capítulo VII.
[1715] Dictamen 01/2012 sobre las propuestas de reforma de la protección de datos, *op. cit.*, pág. 7 y especialmente se analizan los actos delegados en Anexo al Dictamen 8/2012 por el que se proporciona más

a. El establecimiento principal del responsable o del encargado como criterio para determinar la autoridad de control competente

Si bien se deja claro en los tres textos que las autoridades de control serán competentes en el territorio de sus Estados miembros, la dificultad viene en la determinación de la competencia de la autoridad que se considerará principal, en el sistema de ventanilla única, ante tratamientos de datos que llevan a cabo responsables o encargados ubicados en más de un Estado miembro.

La propuesta de la Comisión estableció que, si el tratamiento tenía lugar en el marco de las actividades de un responsable o un encargado, establecido en la UE, y este responsable o encargado tenía establecimientos en varios Estados miembros, la autoridad de control del Estado miembro, donde se ubicara el establecimiento principal del responsable o el encargado, sería la autoridad principal competente para controlar las actividades del responsable o del encargado en todos los Estados miembros (art. 51 PCE-RGPD). Esto sin perjuicio de los mecanismos previstos de cooperación entre las autoridades implicadas. La definición de establecimiento principal era:

> "establecimiento principal: en lo que se refiere al responsable del tratamiento, el lugar de su establecimiento en la Unión en el que se adopten las decisiones principales en cuanto a los fines, condiciones y medios del tratamiento de datos personales; si no se adopta en la Unión decisión alguna en cuanto a los fines, condiciones y medios del tratamiento de datos personales, el establecimiento principal es el lugar en el que tienen lugar las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del responsable del tratamiento en la Unión. Por lo que respecta al encargado del tratamiento, por establecimiento principal se entiende el lugar de su administración central en la Unión" (art. 4.13) PCE-RGPD).

Como puede observarse para determinar el establecimiento principal del responsable se acude a los rasgos que caracterizan el concepto de responsable. De esta forma, en primer lugar, este establecimiento corresponderá al lugar donde se decide sobre los fines, condiciones y medios del tratamiento. Si no se toman estas decisiones en el territorio de la UE, el criterio es similar al adoptado para definir el ámbito de aplicación territorial (art. 3.1 PCE-RGPD). Por tanto, para determinar cual es el establecimiento

información sobre los debates relativos a la reforma de la protección de datos, *op. cit.* y los actos de ejcución en: *Working document 01/2013. Input on the proposed implementing acts, 00166/13/EN WP 200, 22.1.2013, Article 29 Data Protection Working Party.*

principal, habrá que aplicar la metodología seguida para identificar al responsable pero en el marco de sus establecimientos ¿cuál de los establecimientos del responsable es el que decide sobre los fines, condiciones y medios del tratamiento?[1716]

Por otro lado, respecto al encargado del tratamiento, resalta la simplicidad del criterio que se centra en donde tenga lugar su administración central en la UE. Este criterio es coherente con el hecho de que el encargado no decide sobre el tratamiento y, por eso, hay que diferenciar los criterios que se le aplican al encargado de los que se aplican al responsable.

Si bien el GA29 apoyaba el sistema de designación de una autoridad de control principal, llamó la atención sobre la poca claridad de la definición de establecimiento principal y sobre la falta de criterios para determinar la autoridad principal, cuando el responsable o el encargado no tuvieran establecimientos en la UE, en virtud del nuevo ámbito de aplicación territorial del reglamento[1717]. Asimismo, el GA29 indicó que debía quedar claro que la competencia de la autoridad principal no era exclusiva y que debía estar sujeta a las obligaciones de cooperar con otras autoridades implicadas[1718].

El Parlamento modificó esta regulación, de forma que si el tratamiento de datos se produjera en el marco de las actividades de un responsable o de un encargado establecidos en la UE y estuvieran establecidos en varios Estados miembros, o si se trataran los datos personales de residentes en varios Estados miembros, la autoridad principal, que controlaría las actividades de tratamiento en todos los Estados miembros del responsable o del encargado, sería la del Estado miembro donde se situara el establecimiento principal del responsable o del encargado (art. 54bis.1 PPE-RGPD). El

[1716] Hay que recordar que en la propuesta de la Comisión, el responsable determina los fines, las condiciones y los medios del tratamiento pero que luego en los textos del Parlamento y del Consejo UE se eliminó este nuevo aspecto referido a las condiciones del tratamiento.
[1717] Dictamen 01/2012 sobre las propuestas de reforma de la protección de datos, *op. cit.*, pág. 19. RALLO LOMBARTE alertaba sobre la posibilidad de que unas pocas autoridades de control pudieran absorver el ejercicio efectivo de las competencias de control de los otros Estados miembros. Ello se debía a que buena parte de las empresas multinacionales del sector de Internet habían ubicado sus sedes en Irlanda, tanto por la menor presión fiscal de este país, como por la legislación de protección de datos, con un débil régimen sancionador. A. RALLO LOMBARTE, "Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma", *UNED, Revista de derecho político, op. cit.,* pág. 42. Como ejemplo, se puede citar a *Facebook* que, con el fin de evitar la actuación de la autoridad de control belga, alegaba que la filial del grupo, ubicada en Irlanda era la responsable del tratamiento. *Recommandation nº 04/2015 du 13 mai 2015, Comission de la protection de la vie privée, op. cit.*.
[1718] *Ibídem.*

Parlamento reforzó la colaboración entre las autoridades de control y dispuso que el Consejo Europeo de Protección de Datos pudiera emitir un dictamen sobre la determinación de la autoridad principal, en caso de conflicto (art. 54bis.3 PPE-RGPD).

Respecto a la definición de establecimiento principal, el Parlamento también la modificó para entender que era "el lugar donde tenga su establecimiento la empresa o el grupo de empresas en la Unión, ya se trate de un responsable o un encargado del tratamiento, y en el que se adopten las decisiones principales en cuanto a los fines, condiciones y medios del tratamiento de datos personales" (art. 4.13) PPE-RGPD)[1719]. Se añaden en esta definición algunos criterios que ayudarán a determinar este lugar: la localización de las sedes del responsable o del encargado, el emplazamiento de la entidad dentro del grupo de empresas, que esté en mejores condiciones, en términos de abordar y aplicar el reglamento y el emplazamiento en el que se ejerzan de manera efectiva y real las actividades de gestión, que determinen el tratamiento, mediante una instalación estable.

Esta definición merece alguna crítica, ya que, a diferencia de la que establecía la Comisión, se refiere con los mismos criterios al establecimiento de responsables y encargados, pese a que los criterios que alega se refieren claramente a la definición del responsable. Además, no elimina la alusión a las condiciones, aspecto que el Parlamento había eliminado del concepto del responsable. No es coherente con la naturaleza del encargado del tratamiento, que no decide sobre los fines y medios (al menos no sobre los esenciales), que el lugar que debe constituir el establecimiento considerado principal del encargado, sea aquel donde se supone que se decide sobre estos aspectos.

Tampoco se puede dejar de señalar que algunos de los factores que proporciona la definición como ayuda para determinar cual será el establecimiento principal, donde se decide sobre los fines, condiciones y medios del tratamiento, no reflejarían ese poder de decisión. Como ejemplo citar el lugar que sería más adecuado para poder cumplir con las obligaciones del reglamento, criterio totalmente ajeno al poder de decisión.

[1719] Hay que mencionar que la definición se centra en la empresa o grupo de empresas, ya que el texto del Parlamento establece que los tratamientos de datos que lleva a cabo el sector público serán supervisados por las autoridades de los Estados miembros donde se ubique el sujeto de este sector (art. 51.1 PPE-RGPD). Asimismo se incluyen en el texto del Parlamento definiciones de lo que se considera empresa y grupo de empresas (art. 4.15) y .16) PPE-RGPD).

En la resolución del Parlamento se añadió que si el responsable ejerciera también sus actividades como encargado del tratamiento, la autoridad de control del establecimiento principal del responsable actuaría como autoridad principal para el control de las actividades del tratamiento (art. 54bis.3bis PPE-RGPD). Esta previsión resulta confusa, ya que respecto a un concreto tratamiento, no puede considerarse a un sujeto responsable y encargado a la vez.

Por último, el Consejo UE también introduce cambios en la regulación. Las autoridades de control, además de ser competentes en el territorio del Estado miembro donde se ubican, también lo serán cuando el tratamiento lo lleven a cabo autoridades públicas u organismos privados, que actúen en virtud de las bases jurídicas relativas al cumplimiento de una obligación jurídica, o de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamieno (art. 51.2 PCJ-RGPD).

El sistema de designación de una autoridad principal se utilizará, según el texto del Consejo UE, en los casos en los que estemos ante un tratamiento transnacional que engloba, tanto el tratamiento que se produce en el contexto de las actividades de establecimientos en más de un Estado miembro del responsable o del encargado y cuando este responsable o encargado estén establecidos en más de un Estado miembro, como cuando el tratamiento se produzca en el contexto de las actividades de un único establecimiento de un responsable o un encargado en la Unión pero que afecte sustancialmente o es probable que afecte de esta forma a interesados de más de un Estado miembro (art. 4.19ter PCJ-RGPD).

La autoridad principal, en estos casos en los que exista un tratamiento transnacional será la del establecimiento principal o el establecimiento único del responsable o del encargado (art. 51bis.1 PCJ-RGPD). Para determinar el establecimiento principal deberemos acudir a la definición que contiene el texto del Consejo UE que diferencia si se refiere a un responsable o a un encargado (art. 4.13) PCJ-RGPD). El establecimiento principal de un responsable será aquel donde tenga su administración central en la UE, salvo que las decisiones sobre los fines y los medios del tratamiento se adopten en otro establecimiento en la UE que tenga competencias para hacer que se

apliquen las decisiones, por lo que, en este caso, sería este el considerado establecimiento principal.

En caso del encargado del tratamiento, el establecimiento principal también será el lugar de administración central en la UE. Si careciese de administración central en la UE, el establecimiento principal será aquel donde se lleven a cabo las principales actividades del tratamiento en el contexto de las actividades de un establecimiento del encargado, en la medida en la que este encargado esté sujeto a obligaciones específicas, de acuerdo con el reglamento.

Como puede apreciarse, especialmente en el caso del encargado del tratamiento, esta definición de establecimiento es poco clara. A esto hay que añadir que las autoridades de control serán competentes para conocer de reclamaciones o de posibles infracciones del reglamento, si el objeto guarda relación únicamente con un establecimiento situado en su Estado miembro o afecta sustancialmente a interesados en su Estado miembro (art. 51bis.2bis PCJ-RGPD). En este caso, la autoridad de control informará a la autoridad de control principal que decidirá si llevará ella el caso o lo hará la autoridad de control informante (art. 51bis.2ter PCJ-RGPD).

En este sentido, el texto del Consejo UE ha reforzado la colaboración entre todas las autoridades implicadas en un procedimiento de cooperación (art. 54 bis PCJ-RGPD), además de mantener y reforzar los mecanismos que ya se establecían en los textos de la Comisión y el Parlamento: la asistencia mutua (art. 55 PCJ-RGPD), la posibilidad de que realicen las autoridades operaciones conjuntas y el mecanismo de coherencia que se asegura, en última instancia por la adopción de decisiones vinculantes por parte del Consejo Europeo de Protección de Datos, en caso de conflicto entre las autoridades (arts. 57 ss. PCJ-RGPD).

b. El derecho del interesado a presentar una reclamación ante la autoridad de control

El interesado tiene derecho a presentar una reclamación ante la autoridad de control cuando considere que el tratamiento de sus datos no se ajuste a lo establecido en el reglamento (art. 73.1 PCE-RGPD). La Comisión y el Parlamento dispusieron que el interesado pudiera dirigirse a una autoridad de control, en cualquier Estado miembro. El

Consejo UE precisó, en su orientación general, que el interesado podría interponer la reclamación, ante una única autoridad, que podría elegir, en particular, entre las que estuvieran ubicadas en el Estado miembro donde el interesado tuviera su residencia habitual o su lugar de trabajo o donde se hubiera cometido la infracción (art. 73.1 PCJ-RGPD). El añadido de que pudiera elegir en particular entre estas opciones, parece indicar que podría interponer la reclamación ante otras autoridades ubicadas en otros Estados. El Consejo UE también incluyó la necesidad de que la autoridad de control informara al interesado sobre el curso de la reclamación y sobre la posibilidad de interponer recurso judicial (art. 73.5 PCJ-RGPD). Esta obligación de informar también la contemplaban los textos del Parlamento y de la Comisión en la atribución de funciones a las autoridades de control (art. 52.1.b) PCE-RGPD).

2.5.2. Mecanismos procesales

El reglamento, en los tres textos de la Comisión, Parlamento y Consejo UE, se establece la posibilidad de recurrir judicialmente contra una autoridad de control (art. 74 PCE-RGPD) y recurrir judicialmente contra un responsable o encargado (art. 75 PCE-RGPD). Además se establecen estos recursos como un mínimo ya que se indica que es, sin perjuicio de otros recursos que pudieran establecerse.

El reglamento establece el derecho de toda persona física o jurídica a interponer un recurso judicial contra las decisiones de una autoridad de control que le conciernan (art. 74.1 PCE-RGPD). Principalmente irá dirigido, por tanto, a los responsables y encargados del tratamiento afectados por las decisiones de la autoridad de control. El Consejo UE especificó que este recurso debía ser efectivo y contra una decisión que fuera jurídicamente vinculante para esta persona (art. 74.1 PCJ-RGPD). En la parte del preámbulo, el Consejo UE detalló que estas decisiones serían las que afectasen al ejercicio de los poderes de investigación, corrección y autorización de la autoridad de control o a la desestimación o rechazo de las reclamaciones. En cambio, no se consideran decisiones vinculantes otras medidas, como los dictámenes o el asesoramiento que puedan proporcionar las autoridades (Considerando 113 PCJ-RGPD).

El interesado podrá interponer un recurso judicial, con el fin de obligar a la autoridad de control a dar curso a una reclamación, en ausencia de una decisión necesaria

para proteger sus derechos, o en caso de que la autoridad de control no hubiera informado, en el plazo de tres meses, sobre el resultado de una reclamación interpuesta por el interesado (art. 74.2 PCE-RGPD)[1720]. El recurrente debe dirigirse al órgano jurisdiccional del Estado miembro donde esté ubicada la autoridad de control (art. 74.3 PCE-RGPD). Los textos de la Comisión y del Parlamento establecieron que si el interesado no tuviera su residencia habitual en ese Estado, podría solicitar a la autoridad del Estado miembro, donde residiera, que ejercitara, en su nombre, una acción contra la autoridad de control (art. 74.4 PCE-RGPD). El Consejo UE suprimió esta posibilidad.

Los recursos judiciales contra los responsables o encargados podían ser interpuestos por cualquier persona física, según los textos de la Comisión y del Parlamento (art. 75.1 PCE-RGPD) y, por el interesado, en el texto del Consejo UE (art. 75.1 PCJ-RGPD), cuando consideren que los derechos que les brinda el reglamento han sido vulnerados por un tratamiento no conforme con esta norma.

En el caso de los recursos judiciales contra responsables o encargados, el órgano jurisdiccional ante el que debe interponerse el recurso será el de aquel Estado miembro en el que el responsable o el encargado tenga un establecimiento o también el de aquel Estado miembro en el que el interesado tenga su residencia habitual, excepto si es una autoridad pública que actúe en ejercicio de poder público (art. 75.2 PCE-RGPD)[1721].

Se establece claramente la posibilidad de que estos recursos sean interpuestos por organizaciones, organismos o asociaciones que actúen en nombre del interesado. La Comisión y el Consejo UE precisaban que estas entidades debían caracterizarse por tener como objeto la protección de los derechos e intereses de los interesados, por lo que se refiere a la protección de sus datos personales (art. 73.2 PCE-RGPD y 76.1 PCJ-RGPD).

[1720] El Consejo UE matizó que la legislación de la UE o de los Estados miembros podría establecer un plazo menor (art. 74.2 PCJ-RGPD).

[1721] Respecto a esta disposición el GA29 alertaba de que podría ser problemático que se estableciera la posibilidad de interponer acciones ante los órganos jurisdiccionales de cualquier Estado miembro donde tenga un establecimiento el responsable o el encargado independientemente de si éste es un establecimiento principal o no. Además, en el caso de la posibilidad de entablar un proceso contra el responsable ante los órganos jurisdiccionales del Estado miembro, donde tenga la residencia habitual el interesado, pese a que busca beneficiar a éste, puede entrañarle dificultad a la hora de ejecutar la sentencia. Dictamen 01/2012 sobre las propuestas de reforma de la protección de datos, *op. cit.*, pág. 27.

En cambio, el Parlamento sólo exigía que actuaran en interés público (art. 73.2 PPE-RGPD)[1722].

Según los textos de la Comisión y del Parlamento, en el caso de que lo que se interpusiera fuera una reclamación ante la autoridad de control, según se comentaba en el anterior apartado, estas organizaciones, organismos o asociaciones podrían interponerla, por cuenta de uno o más interesados o de forma independiente, de manera que bastaría que consideraran que hay una violación del reglamento[1723]. En los otros casos (recurrir judicialmente contra una autoridad de control, art. 74 PCE-RGPD, y recurrir judicialmente contra un responsable o encargado, art. 75 PCE-RGPD) será necesario que la asociación cuente con la autorización de los interesados. El Consejo UE permitía que estas entidades actuaran en nombre de los interesados, en todos los casos, y dejaba en manos de los Estados miembros la decisión sobre la posibilidad de que actuaran, de forma independiente, para presentar reclamaciones y ejercer los derechos que establecen estos preceptos (art. 76.2 PCJ-RGPD).

En todos los textos se indica a los tribunales nacionales que si tienen conocimiento de que hay en marcha otros procedimientos paralelos relativos a la misma cuestión, podrán suspender el procedimiento (art. 73.3 PCE-RGPD y art. 76bis PCJ-RGPD). El Consejo UE desarrolla esta regulación y precisa que el procedimiento debe versar sobre la misma cuestión que afecte al tratamiento del mismo responsable o encargado (art. 76bis.1 PCJ-RGPD). Asimismo, introduce una prioridad temporal, de forma que el órgano jurisdiccional suspenda si ha conocido posteriormente el asunto (art. 76bis.2bis PCJ-RGPD).

[1722] El cambio realizado en el proceso parlamentario había sido sugerido por el Supervisor Europeo de Protección de Datos en su Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones — «Un enfoque global de la protección de los datos personales en la Unión Europea» (2011/C 181/01) 22.6.2011, pág. 13. También fue sugerido por la Agencia de Derechos Fundamentales de la Unión Europea (FRA). La Agencia proponía ampliar el alcance del precepto de forma que permitiera a entidades con un interés público y, no sólo a entidades en representación de varios titulares de datos, que pudieran interponer acciones ante la justicia. *Avis FRA – 2/2012 de l'Agence des droits fondamentaux de l'Union européenne concernant le programme de réforme des règles en matière de protection des données à caractère personnel, 1 d'octobre 2012*, págs. 6, 28 a 29.

[1723] También se modificó durante el proceso parlamentario esta disposición y, si bien inicialmente, se indicaba en el primer borrador que la violación debía ser de datos personales, se cambió para indicar que la violación era del reglamento (art. 73.3 PPE-RGPD).

El Consejo UE ha incluido, en la parte del preámbulo del reglamento, amplias indicaciones que se dirigen también a los órganos jurisdiccionales nacionales (Considerandos 113 y 114 PCJ-RGPD). De esta forma, les recuerda que pueden interponer cuestión prejudicial ante el TJUE, para que se pronuncie sobre el reglamento. Asimismo, el Consejo UE indica que estos órganos jurisdiccionales no pueden declarar inválida una decisión del Consejo Europeo de Protección de Datos. Cuando el procedimiento se origine contra una decisión de una autoridad de control, que haya sido adoptada para ejecutar una decisión de este órgano, el tribunal deberá remitir la cuestión de la validez al TJUE, de acuerdo con el artículo 267 TFUE.

2.5.3. Responsabilidad civil

En los textos de la Comisión y del Parlamento, se establece el derecho de cualquier persona que sufra un daño ocasionado por una operación de tratamiento ilícito o por un acto incompatible con el reglamento, de recibir una indemnización del responsable o del encargado (art. 77.1 PCE-RGPD). El Consejo UE ha precisado que el daño debe ser ocasionado por una operación de tratamiento que no cumpla con lo establecido en el reglamento (art. 77.1 PCJ-RGPD). Por tanto, el Consejo UE ha restringido el supuesto.

También encontramos en el texto del Consejo UE un desarrollo de la responsabilidad, de forma que se aclara, especialmente, la responsabilidad del encargado. Así se indica que, mientras el responsable implicado en el tratamiento será responsable del daño causado por el tratamiento que no cumpla con el reglamento, el encargado responderá por el daño causado por el tratamiento sólo si no ha cumplido con las obligaciones que el reglamento establece para este y por actuar fuera del ámbito o en contra de las instrucciones del responsable (art. 77.2 PCJ-RGPD).

Tal como se establecía en la Directiva 95/46/CE, el responsable, podrá ser eximido, total o parcialmente, de la responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño (art. 77.3 PCE-RGPD). No obstante a diferencia de la Directiva 95/46/CE, esto también se aplicaría al encargado.

La regulación de la corresponsabilidad se ha ido desarrollando en los diferentes textos. En la propuesta inicial de la Comisión se indicaba que si más de un responsable o

encargado estaban implicados en el tratamiento, cada uno de ellos sería responsable de todo el perjuicio ocasionado (art. 77.2 PCE-RGPD). En el Parlamento se incluyó una excepción a esta responsabilidad total cuando los corresponsables hubieran suscrito un acuerdo por escrito, en el que hubieran determinado sus concretas responsabilidades (art. 77.2 PPE-RGPD). Finalmente, el Consejo UE especificó que, si más de un responsable o encargado, que habían participado en el mismo tratamiento, debía ser considerado responsable, de acuerdo con los criterios ya mencionados, cada uno de ellos debería responder por todo el perjuicio (art. 77.4 PCJ-RGPD). Sin embargo, se añadía la posibilidad de que si uno de los responsables o encargados se hacía cargo del pago de este importe total, podría repetir contra los demás por la parte de la indemnización que correspondiera a sus respectivas responsabilidades (art. 77.5 PCJ-RGPD)

El Parlamento Europeo y el Consejo UE especificaron que los daños serían pecuniarios y no pecuniarios (art. 77.1 PPE-RGPD y PCJ-RGPD).

Al igual que sucedía con los otros recursos comentados, en el caso de este derecho a la indemnización, el Parlamento permitió que el recurso lo interpusiera una entidad que actuara en interés público, aunque, en este caso debía contar con la autorización de los interesados (art. 76.1 PPE-RGPD). El Consejo UE, al igual que la Comisión, no incluyó esta posibilidad. El Consejo UE remite a la regla de competencia establecida para los recursos contra responsables y encargados, ya comentada (art. 77.6 PCJ-RGPD).

2.5.4. La incorporación de un régimen sancionador

Ya desde un primer momento, en el proceso de reforma de la Directiva 95/46/CE, se contempló la necesidad de endurecer las sanciones para reforzar su eficacia[1724]. La primera novedad, por tanto, es que el reglamento contenga un régimen sancionador aunque el enfoque es diferente en los tres textos, especialmente en la caracterización del sujeto infractor.

[1724] La Comisión Europea indicaba como uno de los puntos esenciales el relativo a reforzar la eficacia de las vías de recurso y las sanciones. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, un enfoque global de la protección de los datos personales en la Unión Europea, COM(2010) 609 final, Bruselas, 4.11.2010, pág.10.

La Comisión indicó que los Estados miembros debían establecer las normas sobre las sanciones aplicables a las infracciones que se recogían, de forma pormenorizada (art. 78 PCE-RGPD). Respecto a los sujetos infractores, parecía que se iba a sancionar al responsable, cuando se indicaba que, incluso si no designara a un representante debería cumplir con la sanción o que se sancionaría al representante, sin perjuicio de las sanciones que se promovieran contra el responsable (art. 78.1 y .2 PCE-RGPD). No obstante, el catálogo de infracciones que se incluyó, en el artículo 79 PCE-RGPD, optó por un establecimiento neutro, que se centraba en las conductas infractoras[1725]. Por tanto, las sanciones podían imponerse a las personas físicas o jurídicas, del sector público o privado. En conclusión, será importante a efectos de la imposición de una sanción, la asignación de la obligación que conforma la conducta tipificada como infractora. Adquiere mayor relieve la configuración del estatuto del responsable y, consecuentemente, la asignación de obligaciones al mismo.

Respecto a las sanciones se establecía que deberían ser efectivas, proporcionadas y disuasorias y se incorporaban algunos factores a tener en cuenta en la fijación de la multa[1726]. Ante un primer incumplimiento se disponía la posibilidad de realizar una advertencia escrita, en el caso de personas físicas o empresas u organizaciones con menos de 250 empleados dedicados al tratamiento de datos (art. 79.3 PCE-RGPD). Las multas llegaban hasta 1.000.000.000 euros o el 2 % de su volumen de negocios anual a nivel mundial, lo que incluso supera el régimen español, conocido por su dureza y, que, como se ha visto, sólo llega hasta el máximo de 600.000 euros, máximo que raramente se alcanza.

El Parlamento modificó esta regulación y estableció que, ante el incumplimiento de las obligaciones del reglamento debía imponerse, como mínimo una de las tres sanciones siguientes: la advertencia, la realización de auditorías o una multa de hasta 100.000.000 euros o el 5 % de su volumen de negocios anual a escala mundial en el caso de una empresa, si esta última cifra fuera mayor (art. 79.2.bis PPE-RGPD). Además se añadió una lista de doce criterios para graduar la sanción administrativa (art. 79.2 quater

[1725] Así el artículo 79 apartados 4, 5 y 6 PCE-RGPD, donde se incluyen los tipos infractores, indica que la multa se impondrá "a toda persona que(...)".

[1726] Estos criterios eran la naturaleza, gravedad y duración de la infracción, la intencionalidad o la negligencia, el grado de responsabilidad del sujeto infractor, anteriores infracciones, las medidas adoptadas en función del artículo 23 y la cooperación con la autoridad de control para reparar la infracción (art. 79.2 PCE-RGPD).

PPE-RGPD)[1727]. No obstante, a diferencia de la LOPD, no incluyó criterios que se refirieran específicamente a las características del responsable, con el fin de suavizar las sanciones para las pequeñas empresas, como el volumen de negocio o la actividad. El Parlamento, por tanto, no incluyó un desglose detallado de las infracciones como había hecho la Comisión.

El Consejo UE también modificó la regulación. Además de remitirse a los Estados miembros para que adoptaran las medidas necesarias para garantizar la aplicación de las sanciones, también les dejó que decidieran si se debían imponer multas a las administraciones públicas (art. 79.3ter PCJ-RGPD) e incluso para abstenerse de imponer multas, si las infracciones tipificadas por el reglamento contaran con sanciones penales en su legislación nacional (art. 79.5 PCJ-RGPD).

Las multas se podrían imponer, en lugar o además, de las medidas correctoras que podían adoptar las autoridades de control[1728]. El Consejo UE incluyó, al igual que la Comisión un catálogo de infracciones por tramos, que podían llegar a los mismos importes máximos establecidos por la Comisión (art. 79bis PCJ-RGPD).

Los sujetos infractores en la orientación general del Consejo son el responsable o el encargado. En la concreta infracción no se especifica quien es el sujeto, por lo que debe relacionarse con la asignación de obligaciones en el precepto incumplido.

3. OTRAS REFORMAS E INICIATIVAS INTERNACIONALES

3.1. La reforma del Convenio 108 en el marco del Consejo de Europa

El Convenio 108 fue el primer instrumento de carácter internacional vinculante que incorporó el concepto de responsable, aunque, como vimos, apenas se incorporó en su regulación. Principalmente, se incluía como parte del deber de informar, de manera

[1727] Entre los criterios de graduación se incluye el grado de medidas de carácter técnico y organizativo y los procedimientos aplicados de conformidad con algunas disposiciones que en su mayoría se refieren al principio de *accountability*.

[1728] Estas medidas eran la posible advertencia, la amonestación, la orden de que se atiendan los derechos, la orden de que se realice el tratamiento de acuerdo con el reglamento, la imposición de limitaciones temporales o definitivas al tratamiento y la suspensión de transferencias internacionales de datos (art. 53.1ter PCJ-RGPD).

que el titular de los datos personales tuviera claro ante quién podía dirigirse para ejercer sus derechos. Elaborado en los inicios de los años ochenta, respondió a un contexto de uso incipiente de la informática, que nada tiene que ver con el estado actual de la tecnología.

Por eso, en 2010 se iniciaron los trabajos para modernizar el Convenio 108, que transcurrieron de forma paralela a la reforma de la Directiva 95/46/CE. No es de extrañar, ya que un importante grueso de los Estados parte del Convenio 108, son miembros de la UE e incluso la propia UE[1729]. La coincidencia en el tiempo de estas reformas denota un esfuerzo por lograr una coherencia, entre los instrumentos jurídicos que versan sobre la protección de datos y la necesidad de enfrentarse a la evolución tecnológica[1730]. A finales de 2014, finalizó el proceso de reforma y el Comité creado para llevar a cabo la revisión adoptó un texto, que se revisó en marzo de 2015 (Reforma C108)[1731], con el fin de transmitirlo al Comité de Ministros, para su aprobación. No obstante, el Comité de Ministros ha retrasado su adopción, ya que la UE y la Federación Rusa han realizado reservas[1732].

A raíz del proceso de modernización se concluyó que existía un consenso sobre la necesidad de mantener la neutralidad tecnológica de las disposiciones del Convenio 108, así como su coherencia y compatibilidad con otros instrumentos jurídicos y su carácter abierto que lo potencia como un estándar universal único[1733]. El Convenio 108 pretende instaurar unos principios básicos, de forma que se garantice en el máximo de países participantes una protección mínima para luchar contra la globalización[1734].

[1729] Entre los 47 Estados parte del Convenio, se incluyen los 28 Estados miembro de la UE.

[1730] Así además de la reforma que se lleva a cabo en el ámbito de la UE y del Consejo de Europa, también se pudo ver la la Guía OCDE que finalizó en 2013.

[1731] *Abridged report of the 3rd and final meeting (Strasbourg, 1-3 December 2014), CM(2015)40, Ad hoc Committe on Data Protection (CAHDATA), Council of Europe, Strasbourg, 3 March 2015.*

[1732] La UE ha realizado reservas, con el fin de poder asegurar la coherencia con su propia reforma. *Draft abridged report of the 32nd Plenary meeting (Strasbourg, 1-3 July), T-PD(2015)RAP32Abr_en, Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) (T-PD), Council of Europe, Strasbourg, 2 July 2015,* pág. 2.

[1733] TRONCOSO REIGADA destaca de esta reforma el mantenimiento del carácter abierto del Convenio y la preocupación por asegurar la compatilibidad con la propuesta de reglamento de la UE. A. TRONCOSO REIGADA, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *Revista Española de Derecho Europeo, op. cit.*, págs. 21 a 22. *Draft explanatory report of the modernised version of Convention 108, CASHDATA(2014)06, Council of Europe Ad hoc Committe on data protection (CAHDATA), Council of Europe, Strasbourg, 23 November 2014,* pág. 4.

[1734] *Ibídem.*

El concepto de responsable que se incluye en el nuevo texto es: *“”controller” means the natural or legal person, public authority, service, agency or any other body which alone or jointly with others has the decision-making power with respect to data processing*”, que se podría traducir como: “”responsable” es la persona física o jurídica, autoridad pública, servicio, agencia o cualquier otro organismo, que solo o conjuntamente con otros, tiene el poder de decisión sobre el tratamiento” (art. 2.c) Reforma C108)[1735].

Lo primero que se aprecia es una gran simplificación, al estilo de la definición que veíamos en la Propuesta de Madrid[1736]. Así, se acorta la denominación que pasa a ser “*controller*”[1737] y se elimina el reenvío a la legislación nacional para hallar la competencia del responsable para decidir. También se han suprimido los aspectos concretos sobre los que se reflejaba esta capacidad de decisión (las categorías de datos de carácter personal que debían registrarse y las operaciones a aplicarse) que se limita al tratamiento de datos[1738].

Por tanto, el análisis del concepto tendría como elemento subjetivo prácticamente al mismo, con el único añadido del término “agencia”. Se mantiene la aplicación del Convenio 108 a los sectores público y privado y se especifica que no se aplicará al tratamiento de datos que lleven a cabo individuos con una finalidad personal o doméstica (art. 3 Reforma C108).

[1735] Traducción de la autora.

[1736] Que se menciona como fuente de inspiración. *Draft explanatory report of the modernised version of Convention 108, CASHDATA(2014)06, Council of Europe Ad hoc Committe on data protection (CAHDATA), Council of Europe, Strasbourg, 23 November 2014*, pág. 5.

[1737] Si bien la diferencia no es tan importante respecto a la versión en inglés que era *data controller*. Si bien sólo las versiones inglesa y francesa eran las auténticas, en la versión francesa se denominó al responsable “*maître du fichier*” que se tradujo en la versión española como “autoridad controladora del fichero”.

[1738] En el informe encargado para detectar las lagunas del Convenio 108 respecto al desarrollo tecnológico, se indicaba la necesidad de pasar de un concepto de responsable atado al fichero a un concepto de responsable del tratamiento, de forma que se asociara al ciclo entero del tratamiento. Al respecto, se menciona en el informe la interpretación que realiza el GA29 en su Dictamen 1/2010, sobre las nociones de responsable del tratamiento y encargado del tratamiento. Se alude también al informe explicativo del Convenio 108, que indicaba que debía considerarse responsable al que lo era en última instancia del fichero. Este criterio se considera válido, ya que el responsable debe ser quién realmente tiene control sobre el tratamiento de los datos. La Propuesta de Madrid y al APEC Privacy Framework se mencionan como ejemplo de que se acude a este único criterio relativo a quién decide sobre el tratamiento de datos. J.M. DINANT, C. DE TERWANGNE, J.P. MOINY, *Rapport sur les lacunes de la Convention nº 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques*, Le Bureau du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques (T-PD-BUR) T-PD-BUR(2010)09, CRID, pág. 26.

El elemento objetivo sería el tratamiento de datos (*data processing*). Y es que se modifica la definición de tratamiento automatizado, que pasa a denominarse tratamiento de datos. En la definición se recogen más operaciones de las que se contemplaban anteriormente[1739]. Sin embargo, lo más importante es que incluirá no sólo el tratamiento automatizado, sino también el no automatizado, que deberá realizarse sobre un conjunto de datos estructurado, que sea accesible o se pueda recuperar, de acuerdo con criterios específicos[1740].

El elemento funcional es el poder de decisión (*the decision-making power)* respecto al tratamiento de datos. Según el informe explicativo, el poder de decisión podrá derivar de alguna atribución jurídica o de las circunstancias de hecho[1741]. Para determinar si un sujeto es responsable se señalan algunos factores a tener en cuenta, como el hecho de que este sujeto tenga control sobre: las razones que justifican el tratamiento, los métodos del tratamiento, la selección de los datos tratados o de quien puede acceder a los mismos[1742]. Es decir, estos factores se refieren a los aspectos concretos que se encontraban en la definición anterior del Convenio 108, a los que se añaden los terceros que accedan a los datos[1743].

También se indica que este poder de decisión podrá derivar del hecho de que el tratamiento de datos es la actividad principal del responsable o que el tratamiento es necesario para realizar la actividad principal. Este criterio podría arrojar resultados diferentes a los que resultarían de la interpretación del concepto en la Directiva 95/46/CE[1744]. Y es que pese a que parece haber un mimetismo entre los conceptos, no

[1739] *""data processing" means any operation or set of operations which is performed upon personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data*" (art. 2.c) Reforma C108). Finalmente, se ha introducido la recogida de datos, que no se pudo introducir en el Convenio 108.

[1740] "*Where automated processing is not used, data processing means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria*" (art. 2.c) Reforma C108).

[1741] *Draft explanatory report of the modernised version of Convention 108, CASHDATA(2014)06, Council of Europe Ad hoc Committe on data protection (CAHDATA), Council of Europe, Strasbourg, 23 November 2014*, pág. 9.

[1742] *Ibídem.*

[1743] Al igual que sucedió en la Directiva 95/46/CE, en la que el GA29 interpretó que la simplificación de los aspectos sobre los que decidía el responsable, durante la elaboración de la misma, no significaba que dejaran de tenerse en cuenta. Ver Capítulo II.

[1744] En el informe explicativo se cita como ejemplo una empresa que se dedique al envío de información comercial, cuya actividad principal es el tratamiento de datos. Este sería *a priori* un ejemplo típico de encargado del tratamiento, según los criterios del GA29. También se indica como ejemplo de que el poder

acaban de interpretarse de la misma forma. De nuevo hay que resaltar la importancia de la interpretación en conceptos tan amplios.

Al concepto se le añade el elemento de corresponsabilidad, al igual que figuraba en la Directiva 95/46/CE y se mantiene en el PRGPD "sólo o conjuntamente con otros" (*alone or jointly with others*). Ya el Comité consultivo de la Convención 108, en un informe del año 2007, indicó que la realidad tecnológica mostraba que el modelo en el que una sola entidad es responsable de todos los aspectos del tratamiento automatizado, ya no podía ser considerado suficiente[1745]. El Comité enfatizaba la necesidad de que se retuviera la responsabilidad en un solo sujeto y que si se dieran supuestos de corresponsabilidad, se clarificara la misma o se consideraran a todos los corresponsables responsables de todo el perjuicio[1746].

Así, el Convenio 108 incorpora, en su modernización, la corresponsabilidad y también introduce la definición de encargado del tratamiento (*processor*), que es la persona física o jurídica, autoridad pública, servicio, agencia o cualquier otro organismo que trata datos por cuenta del responsable[1747]. Curiosamente se aclara que el encargado del tratamiento podrá ser, al mismo tiempo, considerado responsable, si trata datos para sus propios fines de forma legítima[1748].

Respecto al estatuto del responsable también hay diferencias respecto al Convenio 108, ya que se han introducido algunas obligaciones de asignación expresa, tanto al

---

de decisión puede derivarse de actividades soportadas por tratamientos de datos, cita el tratamiento de datos de clientes que debe realizar el abogado que los defiende o el tratamiento de datos para ejecutar un contrato. *Draft explanatory report of the modernised version of Convention 108, CASHDATA(2014)06, Council of Europe Ad hoc Committe on data protection (CAHDATA), Council of Europe, Strasbourg, 23 November 2014*, pág. 9.

[1745] *Rapport abrégé de la 23e réunion (Strasbourg 14-16 mars 2007), CM/Inf(2007)24 4 mai 2007, Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE Nº 108)-(T-PD), apdos. 12 a 20*.

[1746] El Comité llegó, por tanto, a la misma interpretación que comentamos del GA29 en lo relativo a los supuestos de corresponsabilidad, interpretación que se ha acogido, como se ha analizado, en el reglamento europeo. *Ibídem*.

[1747] Traducción de la autora del artículo 2.f) Reforma C108: ""*processor" means a natural or legal person, public authority, service, agency or any other body which processes data on behalf of the controller*". También se incluye una definición de destinatario que se incluye en el artículo 2.e) Reforma C108: ""*recipient" means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available"*.

[1748] *Draft explanatory report of the modernised version of Convention 108, CASHDATA(2014)06, Council of Europe Ad hoc Committe on data protection (CAHDATA), Council of Europe, Strasbourg, 23 November 2014*, pág. 9.

responsable, como al encargado del tratamiento[1749]. Así, los Estados parte deberían asegurarse que el responsable cumpla con las obligaciones en materia de medidas de seguridad y notificación de violaciones de datos (art. 7 Reforma C108); información al interesado (art. 7bis Reforma C108) y obligaciones adicionales (art. 8bis Reforma C108). Estas obligaciones adicionales incluyen la obligación general de *accountability*[1750], la realización de evaluaciones de impacto y la adopción de medidas técnicas y organizativas que tengan en cuenta la protección de datos durante todo el ciclo del tratamiento. Respecto al cumplimiento de estas obligaciones adicionales se introduce la necesidad de que los Estados parte tengan en cuenta aspectos como los riesgos para los intereses, derechos y libertades de los interesados, la naturaleza y volumen de los datos, su naturaleza, ámbito de aplicación y fines del tratamiento y el tamaño del responsable o del encargado.

Las otras obligaciones que se entiende se atribuirán también al responsable serán: tratar datos personales respetando los principios de legitimación y calidad (art. 5 Reforma C108) y si son datos considerados sensibles tratarlos de acuerdo con los requisitos establecidos en la legislación (art. 6 Reforma C108), atender el ejercicio de los derechos otorgados a los interesados (art. 8 Reforma C108) y cumplir con los requisitos establecidos por la legislación nacional relativos a las transferencias internacionales de datos (art. 12 Reforma C108).

No hay asignación de derechos o facultades expresa, pero se puede extraer de las obligaciones establecidas[1751]. En lo que se refiere a los recursos, se establece que los

[1749] Al encargado del tratamiento se le asignan expresamente el cumplimiento de las medidas de seguridad (art. 7.1 Reforma C108) y las obligaciones adicionales del artículo 8bis Reforma C108 que se refieren a la *accountability*.

[1750] En el informe explicativo se desglosan algunas medidas que se consideran apropiadas y que deberían adoptar el responsable y el encargado. Entre estas medidas se incluyen las que derivan de la relación entre responsable y encargado como la suscripción de cláusulas contractuales que regulen el encargo para poder cumplir con lo establecido en la convención. También incluyen otras como la formación del personal o el establecimiento de procedimientos internos para posibilitar la verificación y la prueba de cumplimiento, como puede ser la designación de un encargado de protección de datos (*data protection officer*). Este encargado de protección de datos se indica que deberá contar con los medios para actuar con independencia, su designación deberá notificarse a la autoridad de control y podrá ser interno o externo al responsable. *Draft explanatory report of the modernised version of Convention 108, CASHDATA(2014)06, Council of Europe Ad hoc Committe on data protection (CAHDATA), Council of Europe, Strasbourg, 23 November 2014*, pág. 18.

[1751] Así se puede entender que el responsable podrá tratar datos si cuenta con una base jurídica adecuada establecida por ley (art. 5.2 Reforma C108) y podrá tratar categorías especiales de datos si cumple con los requisitos establecidos también por ley (art. 6 Reforma C108). El responsable también podrá tratar datos pese a que se oponga un interesado si demuestra que tiene un interés legítimo para tratar datos que deba

Estados parte adoptarán los recursos y sanciones que sean apropiados contra los incumplimientos de lo establecido en la convención (art. 10 Reforma C108). En el informe explicativo se especifica que, tanto las obligaciones asignadas al responsable, como al encargado del tratamiento y los derechos atribuidos a los interesados deben reflejarse en la adopción de estas sanciones y recursos[1752]. Por tanto, se podrá atribuir responsabilidad tanto al responsable, como al encargado. Serán los Estados parte los que determinarán la naturaleza de las sanciones (civil, administrativa, penal, extrajudicial) y el tipo de recursos[1753].

3.2. La *Consumer Privacy Bill of Rights Act* de los Estados Unidos

Como ya se indicó en el inicio de este trabajo, en febrero de 2012, el presidente de EEUU, Barack Obama, presentaba un conjunto de medidas para incentivar la protección de la privacidad en este país[1754]. Uno de los elementos de esta estrategia era una declaración de derechos sobre la privacidad de los consumidores (*Consumer Privacy Bill of Rights* o CPBR), que debía transformarse en una ley federal. En febrero de 2015, tras tres años de espera[1755], se publicó un borrador de esta ley federal: la *Consumer Privacy Bill of Rights Act of 2015* (CPBRA).

Si bien el sistema de protección que dibuja este borrador de ley mantiene diferencias claras con el sistema europeo, se incluye en el mismo un listado de definiciones que perfila el ámbito de aplicación de la norma. Entre estas definiciones, figura la de entidad incluida (*covered entity*), que aparece como una noción neutra que quiere ayudar a dejar claro el ámbito de aplicación. Así, entidad incluida se define como

---

primar sobre los intereses, derechos y libertades del interesado (art. 8.d Reforma C108). Los responsables podrán beneficiarse de la flexibilidad que podrán establecer los Estados parte respecto a las medidas adicionales del artículo 8bis Reforma C108 relacionadas con la *accountability* (art. 8bis.4 Reforma C108). También podrán beneficiarse de las excepciones y restricciones adoptadas por los Estados parte de acuerdo con lo previsto en el artículo 9 Reforma C108.

[1752] *Draft explanatory report of the modernised version of Convention 108, CASHDATA(2014)06, Council of Europe Ad hoc Committe on data protection (CAHDATA), Council of Europe, Strasbourg, 23 November 2014*, pág. 20.

[1753] *Ibídem*.

[1754] *Consumer data privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf, (fecha consulta: 2.8.2014).

[1755] El 24 de febrero de 2014, cuando se celebraban dos años desde la publicación de la *Consumer Privacy Bill of Rights*, un grupo de entidades remitieron una carta al presidente Obama en la que urgían al mismo a que cumpliera con lo indicado en el documento y convirtiera la *Consumer Privacy Bill of Rights* en una ley. https://epic.org/privacy/Obama-CPBR.pdf (fecha consulta: 2.1.2015).

"una persona que recoge, crea, trata, retiene, utiliza o comunica datos personales en o que afecten al comercio interestatal" (Sec. 4.b.1 CPBRA)[1756].

Hay que tener en cuenta que el borrador pretende fijar una protección mínima para la privacidad de los consumidores y se dirige exclusivamente al sector privado comercial. Esta protección se podrá incrementar con la elaboración de códigos de conducta. Sin embargo, pese a esta restricción a un sector, característica, según vimos, de la protección de la privacidad en EEUU, se trata relativamente de un ámbito más genérico (todo el sector comercial, no sólo una parte de éste). Podría ser esta la razón que ha originado la necesidad de incluir este concepto.

Pero es que si acudimos a otra definición que figura en el borrador, la referida a datos personales (*personal data*), señala que son "aquellos datos que están bajo el control de una entidad incluida y que no están disponibles al público a través de medios lícitos y que se conectan o podrían conectarse por la entidad incluida, a un individuo concreto o se conectan a un dispositivo que está asociado a o que habitualmente lo utiliza un individuo" (Sec. 4.a.1 CPBRA)[1757].

Por tanto, aunque el concepto de entidad incluida, en principio, se refiera a un tratador efectivo de datos personales, el concepto de datos personales exige que estén bajo el control de este sujeto, por lo que parece que encontraríamos el elemento funcional del concepto de la Directiva 95/46/CE.

Pese a esta semejanza, también se han de resaltar las diferencias con la noción de responsable de la Directiva 95/46/CE. Y es que la Directiva 95/46/CE pretende, con este concepto interpretado de forma amplia, acoger a un gran número de organizaciones de todo tipo, lo que se demuestra, por ejemplo, con el extenso elemento subjetivo. En cambio, la definición de la CBPRA, más bien, lo que pretende es servir para excluir algunas organizaciones del ámbito de aplicación de la norma, ya que después de la

[1756] Traducción de la autora: *""Covered entity" means a person that collects, creates, processes, retains, uses, or discloses personal data in or affecting interstate commerce. […]"* (Sec. 4.b.1 CPBRA).
[1757] Traducción de la autora: *""Personal data" means any data that are under the control of a covered entity, not otherwise generally available to the public through lawful means, and are linked, or as a practical matter linkable by the covered entity, to a specific individual, or linked to a device that is associated with or routinely used by an individual[…]"*(Sec. 4.a.1 CPBRA).

definición se incluye un listado extenso de supuestos que se entenderá que no son entidades incluidas.

Así, entre los supuestos excluidos quiero resaltar el que se refiere a:

> "cualquier persona que sin tener conocimiento de ello, recoja, utilice, retenga o comunique cualquier información que se relacione con datos personales y que incluya o que se relacione directamente con la historia clínica de ese individuo, su nacionalidad, su orientación sexual, su identidad de género, creencias religiosas o afiliación; ingresos, bienes o deudas, información sobre geolocalización, datos biométricos o el número de la seguridad social" (Sec. 4.b.1.D.ii CPBRA)[1758].

Este supuesto claramente apunta al factor de la inconsciencia para excluirlo de la aplicación de la normativa. Recordemos que este factor fue descartado por el TJUE, como argumento para entender que el buscador *Google* no era responsable del tratamiento[1759].

Evidentemente, hay otras diferencias importantes con el sistema europeo de protección. En esta norma se fijan unos principios que configuran la base de la protección, que tienen su fundamento en los conocidos como *Fair Information Practice Principles* (FIPPs), que se han adaptado al contexto actual. Estos principios, incluidos en la CBPRA, son: control individual, transparencia, respeto del contexto, seguridad, acceso y exactitud, recogida limitada y *accountability*.

Si bien algunos de estos principios se alinearían, en general, con los que contienen las legislaciones europeas, como el de transparencia, hay que resaltar el principio relativo al "respeto del contexto" y su contraste con el principio de calidad de la Directiva 95/46/CE. El principio de calidad apuntaba a que el responsable debía recoger los datos para finalidades determinadas y no podía dedicarlos posteriormente a finalidades incompatibles con las originarias. El principio de respeto del contexto[1760] especifica que, cuando la entidad incluida no trate los datos personales de forma razonable, en función del contexto, deberá aplicar las salvaguardas que establece la CPBRA (Sec. 103 CPBRA).

[1758] Traducción de la autora: *"Such term does not include […] (D) any person that […] (ii) does not knowingly collect, use, retain, or disclose any information that is linked with personal data and includes, or relates directly to, that individual's medical history; national origin; sexual orientation; gender identity; religious beliefs or affiliation; income, assets, or liabilities; precise geolocation information; unique biometric data; or Social Security number.[…]"* (Sec. 4.b.1.D.ii CPBRA).

[1759] Ver Capítulo VIII.

[1760] Este principio de respeto al contexto es el resultado de fusionar dos de los FIIPs, el principio de concreción de los fines en el momento de la recogida de datos y el de limitación de los fines cuando la empresa mantiene los datos, de forma que sólo puede dedicarlos a los fines originarios.

El contexto se define como las circunstancias que rodean el tratamiento de datos personales que lleva a cabo la entidad incluida (Sec. 4.k) CPBRA)[1761]. Ello no significa que las empresas no puedan utilizar los datos para otros fines incompatibles con los iniciales, sino que, si lo hacen deben aumentar el grado de transparencia y las opciones para que los consumidores puedan ejercer el control. Para ello, se obliga a las entidades incluidas a realizar una gestión de riesgos para la privacidad (*Privacy Risk Management*) (Sec. 103.b) CPBRA). Si las entidades lo que hacen es analizar los datos personales sin respetar el contexto, tampoco deberán aumentar los mecanismos de transparencia, si lo sustituyen por la supervisión de un Consejo de Revisión de la Privacidad (*Privacy Review Board*) (Sec. 103.c) CPBRA).

Hay que destacar también la inclusión del principio de *accountability,* que establece la adopción de medidas por parte de la entidad incluida, para cumplir con las obligaciones de la ley, en virtud de los riesgos para la privacidad asociados a sus prácticas relativas a los datos. Se enuncian algunas de estas medidas como la formación del personal, la evaluación de la protección, la consideración de la privacidad en el diseño de los sistemas y las prácticas y el traspaso de las obligaciones a cualquier persona, a la que la entidad incluida comunique datos (Sec.107.a CPBRA).

Asimismo, hay que hacer mención a las previsiones relativas al establecimiento de indemnizaciones civiles para las entidades incluidas que incumplan los principios (Sec. 203). También comentar la importancia de la autorregulación, de forma que, cuando la entidad incluida se haya adherido a algún código de conducta, si le demandaran por incumplimiento de los principios establecidos en la CPBRA, podrá alegar esta adhesión y, si cumpliera con lo establecido en el código la acción no prosperaría (Sec 301.a.D CPBRA).

[1761] Se incluye un listado no exhaustivo de circunstancias que conformarían este contexto, como los datos que sería previsible que se recogieran para proporcionar un producto o un servicio que el individuo solicitara a la entidad o la edad y el grado de sofisticación de los individuos que usan los productos o servicios de la entidad. Algunos aspectos son subjetivos, como los tipos de datos que se puede prever que podrían tratarse para mejorar un bien o servicio solicitado. Como ejemplo de la divergencia con la regulación europea, se puede mencionar que la AEPD no admitió que el consentimiento del titular de los datos que utilizaba los servicios de *Google* fuera válido, cuando *Google* le informaba que sus datos podrían utilizarse para la mejora de servicios actuales o el desarrollo de nuevos. Asimismo, la AEPD entendió que *Google* combinaba los datos de los diferentes servicios y entendía vulnerado el principio de calidad establecido en el artículo 4 LOPD. Resolución R/02892/2013 de 18 de diciembre de 2013 en Procedimiento nº PS/00345/2013.

Por tanto, las diferencias en los sistemas, planteados en EEUU y en la UE, de protección de la privacidad hacen que sea difícil considerarlos equiparables. Sin embargo, existe una aproximación entre ambos modelos. El nuevo reglamento europeo que sustituirá la Directiva 95/46/CE ha adoptado un enfoque más práctico y preventivo que instaura la opción de la autorresponsabilidad. No obstante, existe una tensión entre este nuevo enfoque y la necesidad de garantizar el núcleo de la protección del derecho. El responsable es imprescindible en la búsqueda de este equilibrio. En EEUU, el proyecto de ley analizado también acude a un concepto más amplio de sujeto obligado, en consonancia con el mayor alcance de la norma. Sin embargo, pese a introducir aspectos similares, el concepto también refleja las diferencias de las opciones legislativas. Por otro lado, la adopción de este proyecto de ley en EEUU evidencia, en cierto modo, que tampoco la autorregulación y la legislación sectorial han sido suficientes[1762].

[1762] TRONCOSO REIGADA, en referencia a la adopción por el presidente Obama de la Consumer Privacy Bill of Rights, en la que se planteaba la autorregulación vinculante pero a la espera de adoptar una ley, entiende que hay un cambio en la posición de EEUU hacia un modelo más normativo. Para este autor esta aproximación al modelo europeo es el reconocimiento de un fracaso, fracaso que también se evidencia en que los países iberoamericanos, en lugar de seguir el modelo norteamericano, siguen el modelo europeo de protección de datos. A. TRONCOSO REIGADA, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *Revista Española de Derecho Europeo*, *op. cit.*, pág. 144.

CONCLUSIONES

1. La génesis del responsable y su relevancia en la regulación europea del derecho a la protección de datos

El concepto de responsable, tal como lo conocemos, tiene su origen en las primeras leyes europeas sobre protección de datos aprobadas en los años setenta. La inclusión de esta definición aparece íntimamente ligada a la opción de estos primeros legisladores, que principalmente se decantaron por utilizar una ley general que se aplicaría de forma transversal a todo tipo de sujetos obligados en cualquier sector. Ello no quiere decir que la estrategia legal de acudir a definiciones para delimitar el ámbito de aplicación sea exclusiva de este tipo de normas generales. Sin embargo, en un sistema regulatorio fundamentado en leyes sectoriales (en lugar de una ley general), como el de EEUU, estas tendrán más acotado su ámbito de aplicación y la definición del sujeto obligado se caracterizará por la descripción más concreta del mismo. Por el contrario, en una norma horizontal adquiere más importancia la definición del sujeto obligado, ya que no puede referirse a características específicas que hagan fácilmente reconocible a dicho sujeto, sino que debe acudirse a factores que, de forma general, puedan individualizarlo.

Ya en estas primeras leyes se apreciaron los principales rasgos definitorios de la figura. Un elemento subjetivo constituido por un amplio abanico de sujetos. Un elemento objetivo que se remitía al ámbito material de las leyes y que evolucionó con el tiempo de un objeto estático (como era el fichero o el banco de datos) a un objeto dinámico (el tratamiento de datos). Y un elemento funcional que se ha erigido en el auténtico elemento caracterizador de la figura del responsable. Mediante este elemento, el concepto se alejaba de la consideración de un sujeto que simplemente actuaba ~~actuara~~ sobre el objeto, un tratador efectivo de los datos, para acercarse al sujeto que ostentaba un poder de control sobre este, si bien en esas primeras leyes dicha capacidad de control aparecía en el concepto solo de una forma implícita. El análisis de esas primeras legislaciones muestra también la capacidad de divergencia que puede llegar a alcanzarse en una regulación con respecto a una misma definición.

Asimismo, el responsable aparece en el Convenio 108, aprobado en el marco del Consejo de Europa, aunque es en la Directiva 95/46/CE donde se le otorga un papel

preponderante en la regulación sobre protección de datos. Asimismo, el concepto de responsable se incluye en los diferentes instrumentos jurídicos adoptados a escala internacional, como la Guía OCDE 2013 o el APEC Privacy Framework.

El concepto de la Directiva 95/46/CE incluye los elementos mencionados y se caracteriza por ser un autónomo, amplio, dinámico y funcional. Al ser un concepto autónomo, la definición de responsable debería poder ser interpretada de forma uniforme, en toda la UE, de acuerdo con el contexto y los objetivos perseguidos por la Directiva 95/46/CE. Sin embargo, la transposición del concepto en las leyes nacionales ha derivado en divergencias que, pese a que tendrían que ser obviadas para respetar esta naturaleza de concepto autónomo no dejan de distorsionar la aplicación del mismo y, consiguientemente, tendrá más dificultades para ser uniforme en toda la Unión.

La centralidad del concepto de responsable en la Directiva 95/46/CE no sólo deriva de su carácter de sujeto obligado, sino también de su contribución a la delimitación del ámbito de aplicación de la norma, de su utilidad como criterio mediante el que se resuelve el conflicto sobre ley aplicable, y como pieza esencial en el sistema de garantías, de forma que responderá ante el incumplimiento de sus obligaciones y se convertirá en necesario garante del derecho.

2. La necesidad de una metodología en la aplicación del concepto y de un sistema completo de asignación de roles

La relevancia del responsable precisa de una aplicación consistente de su concepto en la Directiva 95/46/CE. Esta necesidad ha aflorado especialmente ante la evolución del contexto tecnológico. En el importante asunto *Google*, en sentencia de 13 de mayo de 2014, el TJUE se ha tenido que pronunciar sobre si el buscador debía ser considerado responsable del tratamiento respecto a los datos de otros sitios web a los que enlaza, en las listas de resultados que ofrece a sus usuarios. El tribunal europeo consideró que el objetivo del concepto era la protección eficaz y completa de los interesados, mediante una noción amplia de responsable y entendió que debía incluirse al gestor del motor de búsqueda en la misma. Sin embargo, esta conclusión positiva, que valida la eficacia del concepto, se ve truncada por la falta de aplicación de una metodología sólida al interpretar si se debe considerar que estamos ante un responsable o no. Los efectos de esta

carencia también se ejemplifican en el caso *Google*, mediante la aplicación por parte de la Audiencia Nacional, en sentencia de 29 de diciembre de 2014, de criterios ajenos al concepto para determinar si *Google Spain, S.L.* era responsable.

Otro ejemplo de la importancia de la aplicación del concepto de responsable es la prestación de servicios de *cloud computing*. En este tipo de servicios el prestador, en ocasiones, tiene un elevado control sobre los medios del tratamiento. De entrada, la AEPD y el GA29, mediante una estrategia claramente preventiva, han calificado al prestador de este tipo de servicios como encargado del tratamiento y al cliente de los mismos como responsable. La autoridad de control francesa y el Supervisor Europeo de Protección de Datos han matizado que podrían darse situaciones de control conjunto por parte del prestador y el cliente. Es importante que, en todos los casos en los que se aplique el concepto, se valore la capacidad real de decidir sobre los fines y los medios de todos los sujetos y se asigne la responsabilidad en función de esa realidad.

El resultado del análisis del concepto de responsable es que cumple con su principal objetivo: lograr la protección de los afectados mediante la extensión de la normativa a un amplio número de sujetos obligados. Sin embargo, se aprecian las carencias en la aplicación del mismo que, en consecuencia, minan esta eficacia: se obvia un análisis riguroso centrado en los elementos del concepto y se acude a otros criterios externos al mismo.

Con el fin de suplir estas carencias se propone la utilización de una metodología que principalmente sigue la propuesta por el GA29. El análisis se ha centrado en el concepto de la Directiva 95/46/CE, pero se ha aplicado a los conceptos de las legislaciones nacionales europeas y a los diversos instrumentos jurídicos estudiados, con el fin de ofrecer una panorámica jurídica de esta definición. Como se ha indicado, el concepto se compone de tres elementos: subjetivo, objetivo y funcional. Si se cumplen los requisitos que establecen los tres estaremos ante un sujeto que deberá ser calificado como responsable del tratamiento.

El elemento que caracteriza al responsable y lo diferencia de otros sujetos es el funcional. Este elemento consiste en su capacidad de determinar los fines y los medios del tratamiento de datos. Para dilucidar si nos hallamos ante un responsable, habrá que

acudir a la fuente que brinda al responsable esa capacidad de determinación que puede ser una competencia legal explícita, una competencia implícita que derive de normas o de la práctica jurídica y las circunstancias de hecho. En el análisis tiene que primar la realidad de los hechos por encima de la designación meramente formal del responsable. Ello sin perjuicio de que en algunos ámbitos, como en el del sector público, puede ser necesario que se especifique formalmente quien es el responsable, pero esta designación deberá responder a un efectivo control sobre el tratamiento para no desvirtuar el concepto. En este sentido, debe diferenciarse la determinación del responsable, de la legitimación para tratar datos, aspectos que, en algunas ocasiones se confunden.

En virtud de lo indicado, el reenvío incluido en el concepto de la Directiva 95/46/CE a la legislación nacional, para dejar claro que se puede designar al responsable cuando en esta normativa se establezcan los fines y los medios del tratamiento, resulta a mi juicio no sólo superfluo, sino un factor que ha originado más defectos en la transposición.

Mientras que la determinación de los fines por parte del sujeto deberá activar el rol de responsable automáticamente, en el caso de los medios, será necesario un análisis para verificar si los elementos de los medios sobre los que ejerce esta capacidad de determinación el sujeto se consideran esenciales para el tratamiento o no. Sólo en el primer caso debería considerarse al sujeto como responsable. Los elementos esenciales de los medios, tal como lo interpreta el GA29, deberían ser los que se identificaron en el trámite legislativo que dio lugar a la Directiva 95/46/CE, es decir: los datos personales tratados, las operaciones que se les aplicarán y los terceros que podrán acceder a los datos. Como elementos no esenciales de los medios, estarían los medios técnicos y organizativos utilizados en el tratamiento.

El concepto de responsable se debería ajustar a esta interpretación y debería entenderse que, al indicar “fines y medios”, en realidad lo que se quería decir era “fines o medios”, refiriéndose el término medios a los elementos considerados esenciales en el tratamiento. De este modo, un sujeto sería calificado de responsable si decidiera sobre los fines o sobre los elementos esenciales de los medios del tratamiento.

La Directiva 95/46/CE introdujo, al lado del rol de responsable, el de encargado del tratamiento. Los conceptos de responsable y encargado del tratamiento se completan para extender la protección de los datos a todo el ciclo del tratamiento, sea quien sea el que lo realice. Ante un supuesto de hecho en el que examinemos un concreto tratamiento de datos, deberíamos hallar al sujeto responsable y asignar los papeles a los intervinientes en el tratamiento que podrán ser responsables, encargados del tratamiento, personas que actúan bajo la autoridad de estos o terceros a quienes se comuniquen los datos. La regulación se diseña entorno al ciclo del tratamiento que realiza un responsable, desde que recoge los datos personales hasta que los comunica y, por tanto, salen de su círculo de influencia.

Se podría haber optado por un sistema que asignara la responsabilidad a los tratadores efectivos de los datos. Sin embargo, el modelo es asimétrico, de forma que la responsabilidad principal se asigna al sujeto que gobierna el tratamiento, el responsable, y la responsabilidad secundaria corresponde al tratador efectivo de los datos, que está sometido al primero. El hecho de haber configurado al responsable como el sujeto que decide sobre el tratamiento implica que tiene que haber sujetos que no lo hacen, ya que en caso contrario no tendría utilidad esta diferenciación.

Para poder identificar si estamos ante un encargado del tratamiento, lo más práctico es aplicar los criterios utilizados para identificar al responsable. Si no se puede encontrar la fuente de la capacidad de determinación y se cumplen los elementos del concepto de encargado, habrá que entender que estamos frente a este sujeto. El encargado no tendrá capacidad de determinar los fines y los elementos esenciales de los medios del tratamiento. La aparición de este encargado en el tratamiento se deberá a una decisión del responsable y sobre este recaerá la principal responsabilidad respecto a la actuación del encargado.

Para que el modelo elegido obtenga el efecto deseado de total protección, debería asignarse siempre un rol a todo sujeto que trate o que tenga capacidad de decidir sobre el tratamiento. Pero ¿pueden existir sujetos que queden fuera de estos roles? Un ejemplo es el Considerando 47 Directiva 95/46/CE que da cabida a que el prestador de servicios de comunicaciones electrónicas no tenga asignado ningún papel respecto a los datos que envía a través de sus redes. Esta falta de atribución de rol se compensa con una regulación

sectorial en materia de protección de datos. Sin embargo, no parece que sea conveniente que existan este tipo de supuestos y sería jurídicamente más recomendable seguir un sistema de atribución de roles completo.

3. El régimen singular del responsable de la legislación española

El estudio de las legislaciones nacionales europeas y, especialmente de la ley española, ha permitido ahondar más en la metodología propuesta a raíz del concepto de la Directiva 95/46/CE y al mismo tiempo mostrar las divergencias existentes como fruto de la transposición del concepto. Este análisis puede dar una idea de las dificultades que un responsable ubicado en varios Estados miembros debe enfrentar para adaptarse a las diversas legislaciones.

En este sentido, la LOPD establece claramente en el elemento subjetivo del concepto que podrá ser considerado responsable un ente sin personalidad jurídica incluso en el sector privado, ya que debía admitirse para el sector público cuando se hacía mención al órgano en la definición. Así, la LOPD, a diferencia de la Directiva 95/46/CE, prevé una regulación específica y diferenciada para el sector público y el sector privado. Para determinar cuándo se debe aplicar una u otra regulación deviene fundamental la figura del responsable, pues depende de quién sea este responsable, el fichero se calificará como de titularidad pública o privada y, en consecuencia se le aplicará la regulación específica.

Respecto al elemento objetivo, el concepto se refiere al tratamiento, al igual que la Directiva 95/46/CE. Sin embargo la LOPD denomina al responsable: responsable del fichero o del tratamiento, por lo que, a diferencia de la Directiva 95/46/CE, incluye en el concepto la referencia al fichero.

Por su parte, la LOPD diverge de la Directiva respecto al elemento funcional en los aspectos sobre los que el responsable decide. En la norma española son los fines, contenido y medios del tratamiento (mientras que la Directiva solo menciona los fines y medios). Hay que realizar una interpretación correctora de estos aspectos para entender que deben incluirse todos aquellos que se mencionaron respecto a la definición de la Directiva 95/46/CE. Así, el responsable será el sujeto que decida sobre los fines o los

elementos esenciales de los medios que son: los datos personales tratados, las operaciones que se les aplicarán y los terceros que podrán acceder a los datos. Los elementos no esenciales de los medios son los medios técnicos y organizativos. Sin embargo, la legislación española ha desarrollado las medidas de seguridad que deben aplicarse para garantizar la protección de los datos y se obliga a incluir dichas medidas en el contrato suscrito entre el responsable y el encargado. Por ello, debe entenderse que también tales medidas de seguridad son un elemento esencial de los medios del tratamiento sobre el que debe decidir el responsable.

Otra diferencia que se observa en el concepto de la LOPD respecto al de la Directiva 95/46/CE es que no se ha incluido el reenvío a las leyes para realizar la determinación del responsable cuando estas especifiquen los fines, el contenido y los medios del tratamiento. Esto no obsta para que en un entorno fuertemente regulado, lo habitual sea hallar en la normativa los indicios que nos permitan averiguar si un sujeto tiene capacidad de determinar los fines y los medios de un tratamiento de datos que se derive de lo establecido en esta regulación. Este será especialmente el caso del sector público. También encontramos en algunas regulaciones sectoriales la calificación de los sujetos obligados como responsables o encargados, como sucede en materia de seguros. Sin embargo, no parece la mejor opción designar o calificar al responsable en la normativa sectorial. Si se prima en la determinación del responsable la situación real, la designación formal puede conllevar conflictos ante un contexto evolutivo.

Otros indicios que podrán ayudar a la identificación del responsable son la documentación que se haya elaborado para cumplir con la normativa o para regular el tratamiento de datos en el ámbito interno de la organización, así como la que derive de las relaciones contractuales afectadas por el tratamiento o la documentación que defina la actividad del responsable, como la documentación mercantil.

También hay que destacar, en nuestra regulación, el desarrollo de la figura del encargado del tratamiento, al que se le ha otorgado mayor relevancia, lo que responde a una clara necesidad de adaptarse a la práctica real del extendido uso de la subcontratación. Si bien la LOPD contenía una regulación rígida del encargo, la misma se ha flexibilizado mediante el RLOPD. A este mayor desarrollo de esta institución hay que añadir la atribución de responsabilidad, tanto administrativa, como civil y penal.

La necesidad de proporcionar pautas para diferenciar entre responsable y encargado, cuestión de enorme complejidad y trascendencia, ha implicado la adopción de algunos criterios por la jurisprudencia y la AEPD. El criterio del nuevo vínculo incluido en el RLOPD es un ejemplo, así como la doctrina de los datos adicionales. No obstante, el establecimiento de este criterio se lleva a cabo de forma poco consistente con el concepto de responsable. En vez de precisar que el hecho de que exista un nuevo vínculo entre el titular de los datos y el encargado del tratamiento denotaría que este supuesto encargado podría tener capacidad de decidir sobre los fines, el contenido y los medios del tratamiento, lo que se indica es que existirá comunicación cuando haya este nuevo vínculo con el supuesto encargado. Por otro lado, la doctrina de los datos adicionales estaría en línea con el concepto, al entender que el encargado se convertiría en responsable si decidiera sobre un aspecto considerado esencial: el contenido del tratamiento.

Pero si hay una singularidad en el régimen español del responsable es la creación de la doble figura del responsable: el responsable del fichero y el responsable del tratamiento. Así, pese a que se califique al responsable por su decisión sobre el tratamiento, se ha diferenciado entre estos dos sujetos, de forma que el responsable del fichero sería el que, además de decidir sobre el tratamiento o tratamientos, también decide sobre el fichero que pueda crearse. El responsable del tratamiento sólo decidirá sobre el tratamiento.

La creación de esta doble figura ilustra la trascendencia del proceso legislativo y el efecto que puede tener la elección de una sola palabra. De esta forma, el legislador, al corregir la transposición del concepto en la LOPD, en lugar de optar por sustituir la denominación responsable del fichero por la de responsable del tratamiento, lo que hace es adoptar la de “responsable del fichero o del tratamiento”. En virtud de esta doble mención la jurisprudencia realiza una interpretación mediante la que estima que existen estos dos conceptos de responsable, según el objeto al que se dirige la capacidad de decisión. Esta interpretación se refiere a dos sectores concretos sobre los que hay una regulación específica: los servicios publicitarios y los relativos a la información sobre solvencia patrimonial y crédito.

Si bien parecía que se iba a extender la utilización de esta diferenciación a otros supuestos, como así se interpretó respecto a los usuarios de algunos servicios en Internet o con relación a la videovigilancia, cuando no se graban las imágenes, parece que esta tendencia se ha detenido por parte de la AEPD. La creación de esta doble figura es una muestra de la complejidad que puede llegar a darse en la determinación del responsable y que es fruto de una defectuosa transposición de la Directiva 95/46/CE en nuestro país. También hay que tener en cuenta que la creación de estos dos sujetos implica una modulación de sus obligaciones que estén de acuerdo con sus distintos papeles. Existe el riesgo de que esta diferenciación en las obligaciones derive en una menor protección de los derechos. Así se ilustra con la sentencia del Tribunal Supremo, de 21 de mayo de 2014, en el orden civil, en la que el Alto tribunal considera que no puede existir una modulación de responsabilidades que establezca una disposición reglamentaria y que suponga una restricción del derecho a la protección de datos contraria a toda la regulación multinivel del mismo.

4. Un estatuto complejo

El objetivo de los instrumentos internacionales que regulan la protección de datos, entre los que figura la Directiva 95/46/CE, era principalmente económico. En realidad, lo que querían los Estados era establecer una protección mínima para permitir que los responsables pudieran tratar y comunicar datos en un territorio, sin hallar trabas. Lo que se regula es cómo debe llevarse a cabo el tratamiento para que no vulnere los derechos de los afectados. Por eso, su contenido lo componen principalmente las obligaciones del responsable, aunque también derechos o facultades implícitas en estas obligaciones. Así, el derecho a tratar datos si se cumple con los requisitos establecidos se refleja claramente en la posibilidad que le brinda la Directiva 95/46/CE al responsable de tratar datos en virtud de un interés legítimo que perseguiría fundamentalmente posibilitar el funcionamiento de las empresas, o la posibilidad de tratar datos cuando se deba cumplir una obligación legal o una misión de interés público.

El examen de las obligaciones del responsable en los distintos niveles normativos confirma su gran complejidad, que se amplifica para aquellos sujetos que estén ubicados en más de un Estado miembro de la UE y que tendrán que lidiar con regulaciones diversas. El responsable debe tener en cuenta durante todo el ciclo del tratamiento el

cumplimiento de las diversas obligaciones que no están en todos los casos atribuidas de forma expresa. Para asegurar que el cumplimiento sea coherente debería llevar a cabo un proceso previo de análisis y diseño de la estrategia a adoptar.

En la fase de entrada**,** el responsable debe evaluar a qué base jurídica puede acogerse para realizar el tratamiento, si trata categorías especiales de datos deberá ampararse también en una base jurídica adicional, debe cumplir con el deber de informar a los interesados y notificar la información sobre el tratamiento a la autoridad de control, con el fin de garantizar la publicidad de este a los interesados. En la fase de circulación**,** debe cumplir con los principios de calidad, atender el ejercicio de los derechos que se otorgan a los interesados y cumplir con la obligación de seguridad. En la fase de salida**,** debe respetar lo establecido para el encargo del tratamiento, las comunicaciones de datos y las transferencias internacionales de datos.

De nuevo se pueden mostrar las diferencias que contiene la legislación española con lo establecido en la Directiva 95/46/CE también en lo relativo al estatuto del responsable. En este sentido, el TJUE, en sentencia de 24 de noviembre de 2011, en el asunto *ASNEF*, ha considerado incorrecta la transposición del supuesto relativo al interés legítimo habilitante para tratar datos y se ha tenido que anular el precepto que lo recogía. Asimismo, respecto a la legitimación para tratar datos, la legislación española ha otorgado una clara prevalencia al consentimiento por encima de los otros supuestos y ha admitido que este consentimiento sea tácito, en contra de la interpretación que realiza el GA29.

Otros ejemplos de diferencias con la Directiva 95/46/CE, en la ley española, son: la regulación de los datos especialmente protegidos que se articula de forma independiente a los supuestos de legitimación y el establecimiento de una regulación diferenciada de la comunicación de datos. Respecto al principio de calidad, la AEPD, al contrario que el GA29, ha interpretado que se puede acudir a una base jurídica nueva para poder realizar tratamientos de datos ulteriores con finalidades incompatibles con las inicialmente previstas.

En la legislación española**,** se aprecia un esfuerzo por parte del legislador que, con la aprobación del RLOPD ha intentado en muchos casos corregir algunos aspectos de la transposición de la Directiva 95/46/CE. Por el contrario, no se ha podido corregir algún

precepto heredado de la LORTAD, como el artículo 27 LOPD (relativo a la información sobre la cesión de datos), consecuencia de traslaciones de una ley a otra que, finalmente, hacen muy difícil su aplicación.

5. El responsable ante las tensiones a las que se ve sometido el derecho a la protección de datos

El derecho a la protección de datos se encuentra sometido a una serie de tensiones. El principal factor detonante de las mismas es la evolución tecnológica y la globalización que ha acarreado la misma. La Directiva 95/46/CE se elaboró en una época en la que se había empezado a utilizar Internet y, por tanto, no se podían predecir los avances que se han producido y el cambio social que ha conllevado. El TJUE ha tenido que interpretar la Directiva 95/46/CE para evitar efectos adversos, como en la sentencia de 6 de noviembre de 2003, en el asunto *Lindqvist*, cuando interpretó que a la publicación de datos en Internet no le debía ser aplicada la regulación de las transferencias internacionales. Y es que esta regulación de las transferencias internacionales es un ejemplo de inadaptación al actual contexto. En una sociedad globalizada, donde se realizan transmisiones automáticas de información, los responsables deben atender a unos requisitos muy estrictos.

De nuevo, el factor económico está en juego. Las grandes empresas que han tomado la delantera en el mundo de Internet son principalmente estadounidenses y ello ha originado que muchos de los servicios tecnológicos que utilizan los europeos los prestan estas compañías. Por tanto, sus datos personales son tratados por empresas que tienen otro sistema de protección de los datos no equiparable al europeo. La Decisión *Safe Harbour*, que permitía realizar las transferencias de datos de la UE a las empresas adheridas a la misma, y cuya eficacia ya había sido puesta en duda, quedó aún más dañada por el conocimiento de las filtraciones sobre el espionaje masivo que llevaba a cabo EEUU. Mientras a nivel político la UE negocia con EEUU acuerdos para restaurar la confianza en la protección de datos, el responsable se ha visto de nuevo compelido por el GA29 para que sea él quien adopte cautelas al transferir datos a estas empresas adheridas.

Los criterios establecidos por la Directiva 95/46/CE de resolución de conflictos sobre la ley aplicable han tenido que ser forzados, para poder ampliar su alcance a

responsables ubicados fuera de la UE, por el TJUE en el asunto *Google*, pero, de todas formas, no aseguran una protección completa. Los responsables europeos se encuentran en desventaja porque deben cumplir una legislación más estricta y diversa, pero también quieren aprovechar al máximo las oportunidades económicas que ofrece la tecnología. Se quiere huir de la aplicación de la normativa mediante el uso de tecnologías como las técnicas para anonimizar los datos, mientras el GA29 advierte que debe garantizarse que el anonimato sea irreversible para conseguir escapar de la aplicación de la ley. En este sentido, una decisión relevante que adoptó el TJUE, también en el asunto *Google*, fue el rechazo de la inconsciencia del buscador al tratar datos, como argumento para considerar que no era responsable del tratamiento. Este argumento, que había esgrimido el Abogado General, de haberse aceptado, podría haber supuesto la no responsabilidad en caso de utilización de algoritmos, lo que habría tenido un gran impacto en el fenómeno del análisis de datos del *Big data*.

Igualmente, los responsables se enfrentan a las consecuencias de las diferencias entre los sistemas jurídicos europeo y del *Common Law* lo que se ha ilustrado con el ejemplo de la fase de *pre-trial discovery*. El responsable debe adoptar cautelas y evaluar los datos personales que proporcionará, en virtud de las peticiones que se realicen en esta fase preparatoria del procedimiento judicial, especialmente amplio en los EEUU.

6. El responsable como necesario garante del derecho a la protección de datos en un entorno normativo multinivel

El responsable es, al mismo tiempo, sujeto potencial vulnerador y reparador del derecho de protección de datos. Se puede decir que es quien está en la primera línea tanto de ataque, como de defensa del mismo. Por eso, desde todas las ramas del derecho se le demanda, cada vez más, que se ponga del lado de la reparación y de la protección. Se le pide, se le incita desde la legislación para que sea un sujeto activo y protector, en definitiva, un garante del derecho.

Y es que el responsable es quien está en disposición de proteger el derecho y de hacerlo de la forma más eficaz posible, en el marco de su círculo de influencia, que hay que entender que llega hasta que comunica los datos a otro sujeto. El responsable es quien atenderá las solicitudes de los interesados al ejercer los derechos que les brinda la

regulación y que son el reflejo de su capacidad de control sobre los datos, ya que serán el instrumento más eficaz para protegerlos.

Es evidente que las autoridades de control son una importante garantía de protección, pues deben supervisar el cumplimiento del responsable y perseguirlo si incumple. Sin embargo, quien custodia y maneja los datos es el responsable. Así, el TC admitió y otorgó el amparo a una entidad bancaria que alegaba la vulneración de su derecho a la tutela judicial efectiva en conexión con el derecho de protección de datos (STC 96/2012, de 7 de mayo de 2012). La entidad bancaria había puesto en duda la solicitud de datos personales de sus clientes por un órgano judicial. Ante la alegación de la falta de legitimación activa de la entidad bancaria, el TC recalcó que aunque los datos eran de sus clientes, la entidad era responsable del adecuado tratamiento, uso y custodia de los mismos.

El responsable debe atender a las divergencias existentes, que ya se han apuntado entre las diversas normativas que en materia de protección de datos le puedan aplicar si se ubica en diferentes Estados miembros. También debe tener en cuenta las normativas sectoriales que regulen su actividad. Sin embargo, este nivel de análisis ya no es suficiente y es preciso que el responsable también evalúe si esas normativas cumplen con los requisitos establecidos para limitar este derecho de protección de datos, desde una perspectiva constitucional y de instrumentos supranacionales como son la Carta UE o el CEDH.

La protección efectiva del derecho a la protección de datos demanda del responsable un alto nivel de exigencia y de conocimientos jurídicos. Incluso, a nivel del ordenamiento interno, vemos las diferentes consecuencias y valoraciones de la regulación dependiendo de la rama del derecho desde la cual se evalúe el cumplimiento.

Se ha analizado especialmente la responsabilidad civil en materia de protección de datos establecida en la Directiva 95/46/CE y cómo se ha trasladado a la legislación española. Esta responsabilidad establece el derecho de los interesados a recibir una indemnización en caso de que el incumplimiento del responsable o del encargado del tratamiento de lo establecido en la LOPD causara daños o lesiones a sus bienes o derechos. He defendido que el artículo 19 LOPD -que establece esta disposición- recoge

una regulación específica, típica y que puede ser contractual o extracontractual. De esta forma, entiendo que debe separarse claramente de la regulación que establece la LO 1/1982, si bien es cierto que debido al carácter instrumental del derecho a la protección de datos se pueden acumular ambas regulaciones. Asimismo, el juzgador también puede acudir a los criterios de valoración de los daños que se establecen en la LO 1/1982, al carecer de criterios propios en la regulación de la LOPD.

En caso de ficheros de titularidad pública la responsabilidad se exige de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas, una norma que establece claramente una responsabilidad objetiva. Sin embargo, en la responsabilidad civil, en caso de ficheros de titularidad privada, pese a las posiciones doctrinales que apuntan a la responsabilidad objetiva, entiendo que su determinación exige acudir a la configuración de la obligación que supone el incumplimiento que originará el deber de indemnizar. En función de si esta obligación se puede considerar una obligación de medios o de resultado estaremos ante una responsabilidad civil subjetiva cuasi-objetivada o ante una responsabilidad objetiva, respectivamente. En el primer caso, cabría que el responsable pudiera esgrimir que ha actuado con la diligencia debida. En el segundo caso, el responsable sólo podría alegar que no existe nexo causal entre la conducta incumplidora del responsable y el daño.

En materia de responsabilidad penal, hemos visto que nuestro Código penal establece la protección del derecho a la protección de datos en el artículo 197 ss. CP y que, incluso menciona expresamente al responsable y al encargado en un tipo agravado.

Tanto en la responsabilidad civil, como en la penal, se observa una tendencia hacia la autorresponsabilidad, de forma que se confirma el carácter de garante de los entes colectivos a quienes se otorga la facultad de que se autorregulen. Sin embargo, se trata de una autorregulación regulada, de forma que, aunque se otorgue una cierta libertad para que estas entidades se organicen, se acompaña del establecimiento de unas consecuencias que garanticen la supervisión y el castigo por parte de los poderes públicos en caso de incumplimiento en la adopción de estas medidas.

En cuanto a la responsabilidad administrativa, en la legislación española se contempla un régimen sancionador muy estricto que se atenuó mediante una reforma

realizada en el 2011. El marco sancionador se aplica a responsables y también a encargados del tratamiento y ha sido criticado por no imponer multas económicas a las administraciones públicas.

7. La insuficiencia de la figura del responsable

El derecho a la protección de datos es un derecho eminentemente tecnológico. Por ello, es imprescindible que la tecnología ayude al responsable. De nuevo, la inacción del legislador deja en manos del responsable la responsabilidad de elegir las herramientas tecnológicas que le permitan cumplir con lo establecido en la normativa. Se ha planteado si los desarrolladores de estas herramientas debían incorporarse como sujetos obligados pero parece que sólo en alguna normativa nacional, como en la Ley alemana, se ha dado el paso.

La Directiva 95/46/CE incorporó la obligación de adoptar medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos, en función de los riesgos que afectaran al tratamiento y la naturaleza de los datos. Esta obligación se formulaba con un componente de flexibilidad para el responsable que debía adaptar las medidas al riesgo. Algunas leyes nacionales de protección de datos, como la española, han desarrollado las medidas concretas que el responsable y el encargado deben adoptar.

Sin embargo, en el ámbito de la seguridad de la información, se recurre habitualmente a la estandarización, con el fin de adaptarse a las buenas prácticas en la materia. Por eso, progresivamente desde la UE se ha entendido que debía trabajarse esta vertiente técnica de la protección de datos y se ha incentivado esta normalización, así como la incorporación de principios como la protección de datos desde el diseño o por defecto (*privacy by design* o *by default).* Paralelamente, algunas leyes nacionales y entidades privadas han puesto en marcha sistemas de certificación para los productos y servicios tecnológicos. Este reconocimiento de la necesidad de este enfoque más técnico ha cristalizado con el mandato de la Comisión en 2015 al CEN para iniciar un proceso de estandarización para incorporar la *privacy by design* en los procesos de desarrollo y fabricación de equipos y programas informáticos para proteger la protección de datos. Asimismo, se ha consolidado este enfoque en el proyecto de Reglamento General de Protección de Datos.

8. El concepto de responsable inalterado y un necesario reparto de responsabilidades ante una pluralidad de participantes en el proyecto de reglamento general de protección de datos

La regulación del derecho a la protección de datos se encuentra en un punto de inflexión ante la inminente aprobación del paquete de reforma de las dos principales normas europeas en esta materia: la Directiva 95/46/CE y la Decisión marco 2008/977/JAI. A la relevancia que tendría cualquier cambio de esta legislación, se añade la elección de un instrumento jurídico -como es el reglamento europeo- que persigue la armonización que no consiguió la Directiva 95/46/CE. Sin embargo, pese a que, en principio, la aprobación de un reglamento implicaría el desplazamiento automático de las leyes nacionales, parece que en la orientación general adoptada por el Consejo UE se quiere suavizar este efecto. De esta forma, se incluyen en este texto numerosas remisiones a las leyes nacionales y un mayor margen de maniobra para los Estados miembros frente a los otros textos de la Comisión y el Parlamento.

Esta reforma que se inició en el año 2012 ha tenido un recorrido protagonizado por las presiones de los *lobbies* de grandes empresas y gobiernos, lo que da una idea de la trascendencia de la misma. La protección de datos, principalmente por su calidad de derecho instrumental, se ha convertido en pieza central para proteger a los ciudadanos en el entorno digital. Al ser un espacio global, exige que la protección se dirija no solo a empresas europeas. Por ello, se han adaptado los criterios de aplicación territorial del reglamento para que se extienda a responsables ubicados fuera de la Unión Europea en función de unos puntos de conexión más adaptados a este contexto digital.

Aunque aún no se haya aprobado el texto final del reglamento, parece que el concepto de responsable se conservará intacto respecto al que figuraba en la Directiva 95/46/CE, pese a algunos intentos por modificarlo durante el proceso legislativo. Por lo tanto, se mantiene el reenvío a la legislación nacional o de la UE y la conjunción copulativa “y” en los aspectos concretos a determinar por el responsable.

También se mantiene en el proyecto el papel clave del responsable como delimitador del ámbito de aplicación, como sujeto obligado y como el que debe responder

de sus incumplimientos. Sin embargo, hay algunas variaciones en estos aspectos. De esta forma, el concepto de responsable se utiliza de nuevo como criterio para resolver conflictos, no sólo de ley aplicable en la delimitación del ámbito de aplicación territorial, sino también para determinar la autoridad de control principal en la instauración del sistema de ventanilla única del reglamento. Por otro lado, este papel del responsable, como figura clave de la regulación, lo tendrá que compartir con otro sujeto que ha adquirido mayor importancia: el encargado del tratamiento.

Uno de los aspectos que denotan la evolución normativa para adaptarse al contexto tecnológico es el desarrollo del componente de corresponsabilidad. Los nuevos modelos de negocio que surgen en este contexto son proclives a la intervención de numerosos participantes. Para lograr que se cumpla de forma efectiva lo establecido en el reglamento se ha diseñado un modelo de corresponsabilidad en el que los corresponsables suscribirán un acuerdo para delimitar sus obligaciones y responsabilidades. Sin embargo ¿será esto suficiente ante un entorno que permite interacciones automáticas sin que sea preciso el contacto directo entre los diversos integrantes de los negocios, cuando estos pueden ubicarse en cualquier parte del mundo con diversas sensibilidades por la protección de los derechos?

Es más, de nada servirá desarrollar un modelo de corresponsabilidad si el paso preliminar consistente en la determinación de quién es responsable, no reviste la consistencia jurídica requerida. A ello habrá que añadir la delimitación con el encargado del tratamiento que adquiere en el proyecto de reglamento un papel más importante que en la Directiva 95/46/CE. Al repartir la responsabilidad entre responsable y encargado, se atisban en el proyecto rasgos de independencia del encargado, lo que hace que se difuminen las diferencias entre ambas figuras. Estos signos de independencia del encargado harán más compleja su diferenciación del responsable. Si bien, ya no será tan esencial distinguirlos a efectos de la responsabilidad, hay que tener en cuenta que no responderán de la misma forma, ya que tampoco tendrán las mismas obligaciones.

Otros sujetos que intervienen en la regulación del proyecto de reglamento serán el representante del responsable y el delegado de protección de datos. Estos viejos conocidos que ya aparecían en la Directiva 95/46/CE, tienen en el proyecto un papel más reforzado. El representante, además de tener obligaciones propias en materia de

cooperación con las autoridades, será susceptible de ser sancionado. El delegado de protección de datos tendrá un importante rol en el cumplimiento de las obligaciones del reglamento, si bien habrá que esperar a ver si su designación es obligatoria o no, lo que determinará su verdadera relevancia.

9. La autorresponsabilidad como respuesta al complejo entorno tecnológico

La tendencia hacia un modelo de autorresponsabilidad a la que asistimos en todas las ramas del derecho, ha conducido a su integración en el proyecto de Reglamento General de Protección de Datos, especialmente con el principio de *accountability*. Este principio persigue que el responsable garantice y demuestre el cumplimiento de lo establecido en el reglamento. Sin embargo, habrá que esperar al texto final del reglamento para ver cómo queda perfilado este principio, ya que las instituciones han adoptado diversos enfoques en sus textos, de forma que la Comisión y el Parlamento han apostado definitivamente por su inclusión como principio de protección de datos y por desarrollar ampliamente su regulación. El Consejo UE no lo ha reconocido formalmente como tal, aunque incorpora una regulación mínima, mediante la que deja mayor margen al responsable para utilizar mecanismos de autorregulación.

Independientemente de su reconocimiento como principio de la protección de datos, la *accountability* se encuentra inmersa en muchas de las nuevas obligaciones que contiene el proyecto de reglamento, por lo que es innegable su influencia. Hay que constatar una evolución en la forma de legislar sobre el derecho a la protección de datos. Paralelamente a las obligaciones tradicionales derivadas directamente de los principios materiales y de los derechos de los interesados, se incluyen nuevas obligaciones para el responsable que quieren buscar este enfoque más pragmático y eficiente. Derivado de este nuevo planteamiento, el control *a priori* del cumplimiento de las obligaciones por parte de las autoridades de control se limita y queda en manos del responsable. Se formaliza el necesario proceso reflexivo previo que debe llevar a cabo el responsable mediante nuevas obligaciones como la evaluación de impacto o el análisis de riesgos. El responsable a raíz de los resultados de este proceso previo, será el que tendrá que decidir si consulta a la autoridad de control si considera que el tratamiento conlleva riesgos para los derechos de las personas afectadas.

El responsable deberá asegurarse, mediante la aplicación de los principios de *privacy by design* y *privacy by default*, que adopta medidas para respetar lo establecido por el reglamento en todo el ciclo del tratamiento. Asimismo, estará obligado a documentar el cumplimiento de la regulación y de poner esta documentación a disposición de las autoridades de control. En caso de sufrir un incidente de seguridad deberá ponerlo en conocimiento, tanto de las autoridades como de los interesados.

Los responsables deberán adoptar medidas para cumplir con la normativa y demostrar que las han adoptado, de forma que se facilite la supervisión por parte de las autoridades de control. Se quieren incentivar fórmulas de autorregulación regulada, especialmente códigos de conducta y certificaciones. Pese a que no son mecanismos nuevos, hay una apuesta decidida del legislador por reforzar su utilización por parte del responsable.

El control *a posteriori* se adapta a la naturaleza del nuevo instrumento jurídico y al sistema de ventanilla única. La responsabilidad civil refleja la nueva pluralidad de sujetos obligados, de forma que se amplía a los encargados del tratamiento y a las situaciones de corresponsabilidad. Por último, se introduce un régimen sancionador estricto que habrá que ver si se aplica finalmente al sector público.

Las obligaciones que derivan de las disposiciones materiales también evolucionan, de forma que el abanico de derechos de los interesados se amplía para incidir en aquellos que garantizan el amparo en el nuevo entorno, como el derecho al olvido, la portabilidad o la protección frente a la elaboración de perfiles. Los principios, como la licitud o la calidad, se preservan, aunque se ven sometidos a oscilaciones en los diversos textos, como la base jurídica del consentimiento que permite el tratamiento de datos. En este sentido, la Comisión y el Parlamento estimaron que el consentimiento debía ser explícito, pero el Consejo UE prefiere mantener el carácter de inequívoco. En general, el Consejo UE ha adoptado un enfoque continuista respecto al régimen de la Directiva 95/46/CE, mientras que la Comisión y el Parlamento han querido que se produjera una evolución importante en la regulación.

10. Un futuro lleno de retos donde se pone a prueba el modelo europeo de protección de datos ¿qué papel jugará el responsable?

De la elaboración del proyecto del reglamento se desprenden las dificultades a las que se enfrenta el legislador al querer llevar a cabo una modernización de la regulación. Corremos el peligro de perder algo de la esencia del derecho por el camino con un enfoque orientado a riesgos que no sea respetuoso con los principios nucleares de la protección de datos. En este sentido, el GA29 avisaba que, al evaluar los riesgos, el responsable debe tener en cuenta estos principios materiales.

Al mismo tiempo, las opciones que se barajan en los diferentes textos del procedimiento legislativo respecto a la incorporación del principio de *accountability*, dan una idea del reto que supone este nuevo enfoque. Hay que encontrar un equilibrio entre una solución que esté regulada y, en consecuencia, otorgue seguridad jurídica a todos los implicados, con la flexibilidad que permita al responsable una mayor eficacia y mejor adaptación a su organización del cumplimiento normativo. Al mismo tiempo, el responsable debe ver claro el incentivo de utilizar estos mecanismos de autorregulación. Estos mecanismos deben ser consistentes y no responder a operaciones de maquillaje y debe garantizarse la supervisión y el castigo del incumplimiento. Sólo si se reúnen todos estos aspectos se logrará una estrategia preventiva de cumplimiento, que debe entenderse que es el objetivo de esta regulación.

En este momento parece que nos hallamos en una encrucijada. Por un lado, la UE no quiere seguir perdiendo las oportunidades que proporcionan las tecnologías en una malherida economía, no puede bajar la guardia frente a la amenaza terrorista y está sometida a las presiones de las grandes empresas tecnológicas y los gobiernos, como el de EEUU. Por el otro lado, está la presión de garantizar un modelo europeo que quiere ser paradigma de la protección de los derechos fundamentales. En este sentido, el derecho a la protección de datos se ha convertido en un pilar de la protección en el ámbito digital, ya que su carácter de derecho instrumental garantiza la protección de otros derechos y esto se ha reflejado también en el proyecto de reglamento. Hay que tener en cuenta que el control de los datos implica el control de las personas.

La autorresponsabilidad es una buena respuesta y debe impulsarse. Se deben instaurar mecanismos que procuren enfoques desde la ética que no permitan la actuación automática en nombre de un objetivo económico, cuando estamos poniendo en juego derechos fundamentales de personas que pueden verse perjudicadas. Pero la autorregulación debe ser regulada y, en consecuencia, acompañada de la actuación de control de los poderes públicos. Y es que la autorregulación por sí sola no es la respuesta y, ejemplo de ello, es la tramitación en EEUU de un proyecto de ley largamente reivindicado que regule de forma más amplia la protección de la privacidad.

La protección de datos debería establecerse en un instrumento internacional de alcance mundial que asegurara la protección completa ante este mundo global. Por eso es tan relevante la modernización que, en paralelo a la reforma de la Directiva 95/46/CE en el ámbito de la UE, se ha llevado a cabo del Convenio 108 del Consejo de Europa, convenio que está abierto a todos los Estados, aunque no sean miembros del Consejo.

Sin embargo, a la espera de conseguir ese objetivo, la responsabilidad en el derecho a la protección de datos debería ser una cuestión de todos: ciudadanos, responsables, desarrolladores de tecnología, gobiernos y legisladores. Si algo se puede extraer del relato de la reciente historia del derecho a la protección de datos es que, por mucho que se carguen las tintas en la autorresponsabilidad del responsable o se incida en que los Estados deben respetar los derechos fundamentales en todas sus actuaciones, en definitiva son los ciudadanos quienes pueden marcar la diferencia autoprotegiéndose y haciendo valer sus derechos. En este sentido, se podría reformular la máxima inglesa que entendía que la casa de una persona era su castillo (“*a man’s house as his castle*”) y decir que los datos de una persona, quizás también deberían ser su castillo.

BIBLIOGRAFÍA

ABRIL CAMPOY, J.M., "La prescripción en el derecho civil de Cataluña: ¿es aplicable la normativa catalana solamente cuando existe regulación propia de la pretensión que prescribe?", *InDret* 2/2011 abril, Barcelona, 2011, http://www.indret.com/pdf/817_es.pdf, (fecha consulta: 2.9.2015)

ALONSO GARCÍA, R., *Sistema Jurídico de la Unión Europea*, 2ª ed., Aranzadi, Cizur Menor (Navarra), 2010.

ÁLVAREZ RIGAUDIAS, C., "Las transferencias internacionales de datos personales", TRONCOSO REIGADA, A. (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 1.800 a 1.834.

ALZAGA VILLAAMIL, O., *Comentario sistemático a la Constitución Española de 1978*, Ediciones del Foro, Madrid, 1979.

APARICIO SALOM, J., *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*. 4ª ed., Aranzadi, Cizur Menor (Navarra), 2013.

ARENAS RAMIRO, M., *El derecho fundamental a la protección de datos personales en Europa*, Tirant lo blanch, Valencia, 2006.

-"La protección de datos personales en los países de la Unión Europea", *Revista jurídica de Castilla y León*, nº 16 septiembre 2008, págs. 113 a 168.

-"El derecho de acceso", TRONCOSO REIGADA, A. (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 1.161 a 1.196.

- "La validez del consentimiento en las redes sociales on line", RALLO LOMBARTE, A., MARTÍNEZ MARTÍNEZ, R. (Ed.), VVAA, *Derecho y redes sociales*, 2ª ed., Aranzadi, Cizur Menor (Navarra), 2013, págs. 159 a 201.

ASÚA GONZÁLEZ, C.I., "La responsabilidad(I)", PUIG I FERRIOL, L., GETE-ALONSO Y CALERA, M.C., GIL RODRÍGUEZ, J., HUALDE SÁNCHEZ, J.J. *Manual de derecho civil II, derecho de obligaciones, responsabilidad civil, teoría general del contrato*, Marcial Pons, Madrid, Barcelona, 1998, págs. 455 a 481.

ARROYO YANES, L.M., "Las administraciones públicas y la excepción al principio de prestación del consentimiento por parte del interesado a la recogida y tratamiento de sus datos personales", TRONCOSO REIGADA, A. (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 536 a 560.

BAYO DELGADO, J., "Los artículos 22, 23.1 y 24.1 LOPD", TRONCOSO REIGADA, A. (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 1.341 a 1.350.

BLUMENBERG, A.D., GARCÍA-MORENO, B., "Retos prácticos de la implementación de programas de cumplimiento normativo", MIR PUIG, S., CORCOY BIDASOLO, M., GÓMEZ MARTÍN, V. (Dir.), VVAA, *Responsabilidad de la empresa y compliance. Programas de prevención, detección y reacción penal*, Edisofer, Madrid, 2014, págs. 273 a 300.

BUISÁN GARCÍA, N., "Artículo 18. Tutela de los derechos", LESMES SERRANO, C. (Coord.), VVAA, *La Ley de protección de datos: análisis y comentario de su jurisprudencia*, Lex Nova, Valladolid, 2008, págs. 383 a 394.

BUSTO LAGO, J.M., "La responsabilidad de los responsables de ficheros de datos personales y de los encargados de su tratamiento", *Revista Aranzadi Civil-Mercantil* núm. 5, 2006, págs.1 a 40.

CALVO ROJAS, E., "El régimen sancionador de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. El principio de proporcionalidad", HUERGO LORA, A. (et al.), *La Potestad sancionadora de la Agencia Española de Protección de Datos*, Aranzadi, Agencia Española de Protección de Datos, Cizur Menor (Navarra), 2008, págs. 19 a 31.

CAREY, P., *Data protection. A practical guide to UK and EU Law*, 3rd ed., Oxford University Press, Oxford, 2009.

CARR, N. G., "The end of corporate computing", *MIT Sloan management review*, April, 2005. http://sloanreview.mit.edu/article/the-end-of-corporate-computing/ (fecha consulta: 9.9.2014).

CARRILLO, M., "La objetivación del recurso de amparo: una nueva vía de garantía jurisdiccional de los derechos", CARRILLO, M., ROMBOLI, R., *La reforma del recurso de amparo*, Fundación Coloquio Jurídico Europeo, Madrid, 2012, págs. 13 a 80.

CASADO CADARSO, M.T., VILA MUNTAL, M.A., "Los ficheros de las Fuerzas y Cuerpos de Seguridad", TRONCOSO REIGADA, A. (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 1.388 a 1.408.

CAVOUKIAN, A., *Privacy by design… Take the challenge*, Information and Privacy Commissioner of Ontario, Ontario, 2009.

CERRILLO I MARTÍNEZ, A., "Comunicación de datos entre administraciones públicas", TRONCOSO REIGADA, A. (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 1.207 a 1.327.

DARNACULLETA I GARDELLA, M.M., *Autorregulación y derecho público: la autorregulación regulada*, Marcial Pons, Madrid, 2005.

DAVARA FERNÁNDEZ DE MARCOS, I., *Hacia la estandarización de la protección de datos personales. Propuesta sobre una "tercera vía o tertium genus" internacional*, La Ley, Las Rozas (Madrid), 2011.

DAVARA RODRÍGUEZ, M. A., *La Protección de datos en Europa: principios, derechos y procedimiento*, Grupo Asnef- Equifax, Madrid, 1998.

- "El concepto de fichero en la normativa sobre protección de datos", TRONCOSO REIGADA, A. (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 213 a 226.

DE ÁNGEL YAGÜEZ, R., "La responsabilidad civil. Cuestiones previas de delimitación", SIERRA GIL DE LA CUESTA, I., DE ÁNGEL YAGÜEZ, R. [et al.] (Coord.), VVAA, *Tratado de responsabilidad civil*, *Tomo I*, Bosch, Barcelona, 2008, págs. 3 a 123.

-"Fundamento de la responsabilidad civil. Culpa y riesgo. Responsabilidad objetiva. Regímenes especiales de responsabilidad", SIERRA GIL DE LA CUESTA, I., DE ÁNGEL YAGÜEZ, R. [et al.] (Coord.), VVAA, *Tratado de responsabilidad civil, Tomo I*, Bosch, Barcelona, 2008, págs. 125 a 218.

DE ASÍS ROIG, A.E., GÓNZALEZ ESPADA, F.J., "Tipos de infracciones", TRONCOSO REIGADA, A. (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 2.038 a 2.133.

DE HERT, P., STEFANATOU, D., "The accountability culture in its european unión dress. Sticks but no carrots to make the proposed data protection regulation work", RALLO LOMBARTE, A., GARCÍA MAHAMUT, R. (Ed.), VVAA, *Hacia un nuevo derecho europeo de protección de datos. Towards a new European data protection regime*, Tirant lo Blanch, Valencia, 2015, págs. 389 a 410.

DEL CASTILLO VÁZQUEZ, I.C., *Protección de datos: cuestiones constitucionales y administrativas. El derecho a saber y la obligación de callar*, Civitas, Madrid, 2007.

DEL PESO NAVARRO, E., "La figura del responsable del fichero de datos de carácter personal en la LORTAD." *Informática y derecho: Revista iberoamericana de derecho informático*, Nº 6-7, 1994, pp. 249 a 270.

- *Ley de Protección de Datos: la nueva LORTAD*. Díaz de Santos, Madrid, 2000.

DEL PESO NAVARRO, E., RAMOS GONZÁLEZ, M.A., *Confidencialidad y seguridad de la información: la LORTAD y sus significaciones socioeconómicas*, Díaz de Santos, Madrid, 1994.

- *Lortad: análisis de la ley*, Díaz de Santos, Madrid, 1998.

DEL PESO NAVARRO, E., RAMOS GONZÁLEZ, M.A., DEL PESO RUÍZ, M., DEL PESO RUÍZ, M., *Nuevo reglamento de protección de datos de carácter personal. Medidas de seguridad*, Díaz de Santos, Madrid, 2008.

DE LA CUEVA GONZÁLEZ-COTERA, J., "Relato del VII Congreso Internacional sobre Internet, Derecho y Política: Neutralidad de la red y derecho al olvido", *Revista de Internet, Derecho y Política*, nº 13, Febrero 2012, págs. 84 a 90.

DENNINGER, E., "El derecho a la autodeterminación informativa", trad. cast. de PÉREZ LUÑO, A.E., PÉREZ LUÑO, A.E. (Dir.), VVAA, *Problemas actuales de la documentación y la informática jurídica, Actas del Coloquio Internacional celebrado en la Universidad de Sevilla, 5 y 6 de marzo de 1986*, Fundación Cultural Enrique Luño Peña, Madrid, 1987, págs. 268 a 276.

DESBIEY, O., "Le quantified self au coeur des nouvelles pratiques numériques de santé", *IP Innovation & Prospective*, nº 5 juillet 2013.

DHONT, J., PEREZ V., POULLET, Y. y REIDENBERG, J., BYGRAVE, L., *Safe harbour decision implementation study, at the request of the European Commission, Internal Market DG, Contract PRS/2003/A0-7002/E/27*, 2004, http://ec.europa.eu/justice/policies/privacy/docs/studies/safe-harbour-2004_en.pdf (fecha consulta: 23.7.2013).

DÍAZ CREGO, M., *Protección de los derechos fundamentales en la Unión Europea y en los Estados miembros*, Reus, Madrid, 2009.

DÍAZ REVORIO, F.J., "Derecho de la información en la recogida de datos. Una perspectiva constitucional", TRONCOSO REIGADA, A. (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 433 a 451.

DÍEZ-PICAZO, L.M., *Sistema de derechos fundamentales*, 4ª ed., Aranzadi, Cizur Menor (Navarra), 2013.

DÍEZ-PICAZO, L., *Fundamentos del derecho civil patrimonial. V La responsabilidad civil extracontractual*, Aranzadi, Cizur Menor (Navarra), 2011.

DINANT, J.M., DE TERWANGNE, C., MOINY, J.P., *Rapport sur les lacunes de la Convention nº 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques*, Le Bureau du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques (T-PD-BUR) T-PD-BUR(2010)09, CRID.

EGUSQUIZA BALMASEDA, M. A., "Aspectos civiles de la protección de datos", *Publicaciones del Consejo General del Poder Judicial: Monografías. Cuadernos digitales de Formación. Recursos electrónicos*, CGPJ nº29, Madrid, 2012.

ELGUERO, J.M., "El seguro de responsabilidad civil por protección de datos personales", *Revista de responsabilidad civil y seguro*, págs. 47 a 80 http://www.asociacionabogadosrcs.org/doctrina/doctrina02.pdf?phpMyAdmin=9eb1fd7fe71cf931d588191bc9123527 (fecha consulta: 16.7.2015).

FARRÉ TOUS, S., "El encargado del tratamiento en el ámbito de las administraciones públicas", TRONCOSO REIGADA, A. (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 1.103 a 1.126.

FERNÁNDEZ LÓPEZ, J.M., "Principio de consentimiento", TRONCOSO REIGADA, A. (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 453 a 473.

FERNÁNDEZ SALMERÓN, M., *La protección de los datos personales en las Administraciones Públicas*, Civitas, Madrid, 2003.

FREIXES, T., GALLARDO, A., VALLVÉ, Z., *FRANET, Contractor Ad hoc Information Report, Data protection: redress mechanisms and their use, Spain*, Movimiento por la Paz (MPDL), Gabinet d'Estudis Socials (GES), Instituto Europeo de Derecho (IED), 2012.

FREIXES SANJUAN, T., "Els drets fonamentals en perspectiva multinivell. Reflexions entorn dels seus efectes", *Revista catalana de dret públic*, núm. 50, (juny 2015), págs. 32 a 41.

FROSINI, V., *Cibernética, derecho y sociedad*, Tecnos, Madrid, 1982.

-"La Convenzioni europea sulla protezione dei dati*", Rivista di diritto europeo, Anno XXIV nº 1 Gennaio-Marzo 1984*.

GARCÍA DEL POYO VIZCAYA, R., "Encargado del tratamiento", TRONCOSO REIGADA, A. (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 1.081 a 1.102.

GARCÍA MORALES, M.J., "La regulación de los servicios multimedia en Alemania", *Autonomies*, núm. 25, 1999, págs. 37 a 66.

-"Poderes públicos, autorregulación y protección del consumidor en Internet: a propósito de la regulación del distintivo público de confianza", COTINO HUESO, L. (Coord.) VVAA, *Consumidores y usuarios ante las tecnologías*, Tirant lo Blanch, Valencia, 2008, págs. 256 a 282.

-"Libertad de expresión y control de contenidos en internet", CASANOVAS ROMEU, P., *Internet y pluralismo jurídico: Formas emergentes de regulación,* Comares, Granada, 2003, págs. 33 a 69.

-"La prohibición de la censura en la era digital", *Teoría y realidad constitucional*, núm. 31, 2013, págs. 237 a 276.

GEIJO CASTANYA, M., "Prestación de servicios de información sobre solvencia patrimonial y crédito", TRONCOSO REIGADA, A. (Dir.). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal.* Aranzadi, Cizur Menor (Navarra), 2010, págs. 1.579 a 1.624.

GÓMEZ CALLE, E., "Capítulo VI. Los sujetos de la responsabilidad civil. La responsabilidad por hecho ajeno", REGLERO CAMPOS, L.F. (Coord.), VVAA, *Tratado de responsabilidad civil, Tomo I Parte General,* 4ª ed., Aranzadi, Cizur Menor (Navarra), 2008, págs. 931 a 1.066.

GÓMEZ-JARA DÍEZ, C., "Capítulo V. Fundamentos de la responsabilidad penal de las personas jurídicas", BAJO FERNÁNDEZ, M., FEIJOO SÁNCHEZ, B.J., GÓMEZ-JARA DÍEZ, C., *Tratado de responsabilidad penal de las personas jurídicas,* Aranzadi, Cizur Menor (Navarra), 2012, págs. 109 a 133.

GÓMEZ NAVAJAS, J., *La protección de los datos personales: un análisis desde la perspectiva del derecho penal*, Aranzadi, Cizur Menor (Navarra), 2005.

GRIMALT SERVERA, P., *La responsabilidad civil en el tratamiento automatizado de datos personales*, Comares, Granada, 1999.

-"La necesaria reconducción del régimen jurídico de la protección de los datos personales desde la perspectiva de los conflictos y solapamientos con otros derechos y libertades en internet", VALERO TORRIJOS, J. (Coord), VVAA, *La protección de los datos personales en internet ante la innovación tecnológica. Riesgos, amenazas y respuestas desde la perspectiva jurídica,* Aranzadi, Cizur Menor (Navarra), 2013, págs. 65 a 87.

GUASCH PORTAS, V., *Las transferencias internacionales de datos en la normativa española y comunitaria*, Agencia Española de Protección de Datos, BOE, Madrid, 2014.

GUERRERO PICÓ, M. C., *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal,* Aranzadi, Cizur Menor (Navarra), 2006.

GUERRERO ZAPLANA, J., "Artículo 43. Responsables", LESMES SERRANO, C. (Coord.), VVAA, *La Ley de protección de datos: análisis y comentario de su jurisprudencia*, Lex Nova, Valladolid, 2008, págs. 625 a 632.

GUTIÉRREZ ESPADA, C., CEVELL HORTAL, M.J., PIERNAS LÓPEZ, J.J., GARCIANDÍA GARMENDIA, R., *La Unión Europea y su derecho*, Trotta, Madrid, 2012.

HEREDERO HIGUERAS, M., *La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (Comentarios y textos)*, Tecnos, Madrid, 1996.

- *La Directiva comunitaria de protección de los datos de carácter personal (Comentario a la Directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos)*, Aranzadi, Cizur Menor (Navarra), 1997.

-"Ensayo sobre la regulación de la responsabilidad y administrativa en la LO 15/1999 de protección de datos de carácter personal", TRONCOSO REIGADA, A. (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 2.178 a 2.187.

HERNÁNDEZ LÓPEZ, J.M., *El derecho a la protección de datos personales en la doctrina del Tribunal Constitucional*, Aranzadi, Cizur Menor (Navarra), 2013.

HERRÁN ORTIZ, A.I., *El Derecho a la intimidad en la nueva ley orgánica de protección de datos personales*, Dykinson, Madrid, 2002.

HOLMES, N. *Canada's Federal Privacy Laws*, PRB 07-44E, *Law and government division, revised 25 September 2008*, http://www.parl.gc.ca/Content/LOP/researchpublications/prb0744-f.htm (fecha consulta: 5.08.2014).

IGUALADA MENOR, Á., "Creación, modificación o supresión de ficheros de titularidad pública", TRONCOSO REIGADA, A. (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 1.288 a 1.306.

KUNER, C., *European data protection law, corporate compliance and regulation*, 2nd ed., Oxford University Press, Oxford, 2007.

LAFFAIRE, M.L., *Protection des données à caractère personnel*, Éditions d'Organisation, Paris, France, 2005.

LAGUNA REYES, L., *Responsabilidad civil derivada de la inclusión indebida en un registro de morosos*, Trabajo fin de Máster Universitario Acceso a la Abogacía, ARCOS VIEIRA, M.L. (Directora), Universidad Pública de Navarra, 2014, http://hdl.handle.net/2454/9628, (fecha consulta: 10.7.2014).

LESMES SERRANO, C. (Coord.), VVAA, *La Ley de protección de datos: análisis y comentario de su jurisprudencia*, Lex Nova, Valladolid, 2008.

LESSIG, L., *Code, version 2.0.*, *Basic Books*, USA, 2006

LINDE PANIAGUA, E., BACIGALUPO SAGGESE, M., FUENTETAJA PASTOR, J.A., *Principios de Derecho de la Unión Europeo,* 4ª ed., Constitución y Leyes, Madrid, 2011.

LÓPEZ AGUILAR, J.F., "Data protection package y Parlamento europeo", RALLO LOMBARTE, A., GARCÍA MAHAMUT, R. (Ed.), VVAA, *Hacia un nuevo derecho europeo de protección de datos. Towards a new European data protection regime*, Tirant lo Blanch, Valencia, 2015, págs. 29 a 81.

LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa (La protección de los datos personales frente al uso de la informática)*, Tecnos, Madrid, 1990.

- *Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal)*, Centro de Estudios Constitucionales, Madrid, 1993.

-"La primera jurisprudencia sobre el derecho a la autodeterminación informativa", *Datospersonales.org*, nº 1, Marzo 2003.

LLÁCER MATACÁS, M. R., *La autorización al tratamiento de información personal en la contratación de bienes y servicios. La privacidad, entre el estatuto del responsable y la fragilidad del consentimiento*, Dykinson, Madrid, 2012.

MALUQUER DE MOTES BERNET, C., "Códigos de conducta y buenas prácticas en la gestión de datos personales", LLÁCER MATACÁS, M.R., *Protección de datos personales en la sociedad de la información y la vigilancia*, La Ley, Las Rozas (Madrid), 2011, págs. 118 a 132.

MARTÍNEZ MARTÍNEZ, R. *Una aproximación crítica a la autodeterminación informativa.* Civitas, Madrid, 2004.

- "El derecho y el cloud computing", MARTÍNEZ MARTÍNEZ, R.(Ed.), VVAA, *Derecho y cloud computing*, Aranzadi, Cizur Menor (Navarra), 2012, págs. 15 a 36.

- "El complejo encaje normativo de la propuesta de Reglamento general de protección de Datos de la Unión Europea", *Actualidad jurídica Aranzadi*,nº 839, 2012, pág. 3.

- "Menores y redes sociales. Condiciones para el cumplimiento del artículo 13 del Reglamento de desarrollo de la Ley Orgánica de protección de datos", RALLO LOMBARTE, A., MARTÍNEZ MARTÍNEZ, R. (Ed.) VVAA, *Derecho y redes sociales*, 2ª ed., Aranzadi, Cizur Menor (Navarra), 2013, págs. 202 a 230.

- *Olvidar es un fenómeno muy complejo*, 14.5.2014 http://lopdyseguridad.es/olvidar-es-un-fenomeno-muy-complejo/ (fecha consulta: 21.8.2015).

MARTOS DÍAZ, N., CASADO OLIVA, O., "Políticas de privacidad, redes socials y protección de datos. El problema de la verificación de edad. Sistemas de autorregulación", RALLO LOMBARTE, A., MARTÍNEZ MARTÍNEZ, R. (Ed.) VVAA, *Derecho y redes sociales*, 2ª ed., Aranzadi, Cizur Menor (Navarra), 2013, págs. 231-256.

MELL, P., GRANCE, T., *The NIST definition of cloud computing, Recommendations of the National Institute of Standards and Technology, Special Publication 800-145 September 2011, NIST, U.S. Department of Commerce*.

MERCADO PACHECO, P., "Artículo 16. Libertad de empresa", MONEREO ATIENZA, C., MONEREO PÉREZ, J.L. (Dir. Coord.), VVAA, *La Europa de los derechos. Estudio sistemático de la Carta de los derechos fundamentales de la Unión Europea*, Comares, Granada, 2012, págs. 375 a 400.

MESSÍA DE LA CERDA BALLESTEROS, J.A., *La Cesión o comunicación de datos de carácter personal*, Aranzadi, Cizur Menor (Navarra), 2003.

MILLER, A.R., *The Assault on Privacy*, The University of Michigan Press, EEUU, 1971.

MIR PUIG, S., "Las nuevas "penas" para personas jurídicas: una clase de "penas" sin culpabilidad", MIR PUIG, S., CORCOY BIDASOLO, M., GÓMEZ MARTÍN, V. (Dir.), VVAA, *Responsabilidad de la empresa y compliance. Programas de prevención, detección y reacción penal*, Edisofer, Madrid, 2014, págs. 3 a 14.

MITJANS PERELLÓ, E., "Impacto de la entrada en vigor del reglamento de desarrollo de la LOPD en el ámbito de actuación de la Agencia Catalana de Protección de Datos", TRONCOSO REIGADA, A. (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 1.976 a 1.992.

- "El modelo de protección de datos de la Ley 32/2010, de 1 de octubre de 2010, de la Autoridad Catalana de Protección de Datos", *Comunicaciones en propiedad industrial y derecho de la competencia*, nº 63, 2011, págs. 7 a 25.

MORALES PRATS, F., "Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", QUINTERO OLIVARES, G. (Dir.), MORALES PRATS, F. (Coord.), VVAA, *Comentarios a la Parte Especial del Derecho Penal*, 8ª Ed., Aranzadi, Cizur Menor (Navarra), 2009, págs. 401 a 466.

MORENILLA ALLARD, P., "Tutela procesal civil de los derechos fundamentales", GIMENO SENDRA, V., MORENILLA ALLARD, P., *Los procesos de amparo. Civil, penal, administrativo, laboral, constitucional y europeo*, 3ª ed., Colex, Madrid, 2014, págs. 19 a 42.

- "La demanda de amparo ante el Tribunal Europeo de Derechos Humanos (I)", GIMENO SENDRA, V., MORENILLA ALLARD, P., *Los procesos de amparo. Civil, penal, administrativo, laboral, constitucional y europeo*, 3ª ed., Colex, Madrid, 2014, págs. 201 a 230.

- "La demanda de amparo ante el Tribunal Europeo de Derechos Humanos (II)", GIMENO SENDRA, V., MORENILLA ALLARD, P., *Los procesos de amparo. Civil, penal, administrativo, laboral, constitucional y europeo*, 3ª ed., Colex, Madrid, 2014, págs. 231 a 263.

NICOLAS JIMÉNEZ, P., "Ficheros policiales de perfiles de ADN", TRONCOSO REIGADA, A. (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 1.429 a 1.455.

NIEVES SALDAÑA, M., "The right to privacy. La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis", *Revista de Derecho Político* (UNED), núm. 85-2012, págs. 195 a 240.

O'CALLAGHAN MUÑOZ, X. "La responsabilidad objetiva", MORENO MARTÍNEZ, J.A. (Coord.), VVAA, *La responsabilidad civil y su problemática actual*, Dykinson, Madrid, 2007, págs. 800 a 820.

ORDÓÑEZ SOLÍS, D., *Privacidad y protección judicial de los datos personales*, Bosch, Barcelona, 2011.

ORTEGA GIMÉNEZ, A., "Cloud computing, protección de datos y derecho internacional privado (resolución de controversias y determinación de la ley aplicable)", R. MARTÍNEZ MARTÍNEZ (Ed.), *Derecho y cloud computing*, Aranzadi, Cizur Menor (Navarra), 2012, págs. 255 a 287.

ORTÍ VALLEJO, A., *Derecho a la intimidad e informática (Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada)*, Comares, Granada,1994.

ORTIZ DE URBINA GIMENO, I., "Responsabilidad penal de las personas jurídicas: *the american way*", MIR PUIG, S., CORCOY BIDASOLO, M., GÓMEZ MARTÍN, V. (Dir.), *Responsabilidad de la empresa y compliance. Programas de prevención, detección y reacción penal*, Edisofer, Madrid, 2014, págs. 35 a 85.

PALOMAR OLMEDA, A., "Obligaciones previas al tratamiento de datos", MARTÍNEZ MARTÍNEZ, R. (coord.), VVAA, *Protección de datos: comentarios a la LOPD y su reglamento de desarrollo*, Tirant lo Blanch, Valencia, 2009, págs. 63 a 88.

PANTALEÓN PRIETO, F., "Cómo repensar la responsabilidad civil extracontractual (También la de las Administraciones Públicas)", DE ÁNGEL YÁGÜEZ, R., YZQUIERDO TOLSADA, M. (Coord.), VVAA, *Estudios de responsabilidad civil en homenaje al profesor Roberto López Cabana*, Dykinson, Madrid, 2001, págs. 189 a 216.

PARDO LÓPEZ, M. M., "No sólo protección de datos personales en internet: de los conceptos jurídicos híbridos, las categorías mutantes y otras evoluciones en curso", VALERO TORRIJOS, J. (Coord), *La protección de los datos personales en internet ante la innovación tecnológica. Riesgos, amenazas y respuestas desde la perspectiva jurídica*, Aranzadi, Cizur Menor (Navarra), 2013, pags. 89 a 112.

PEGUERA POCH, M., *La exclusión de responsabilidad de los intermediarios en Internet*, Comares, Granada, 2007.

PENDÓN MELÉNDEZ, M.A., GÁLLEGO HIGUERAS, G.F., "Tratamientos con fines de publicidad y de prospección comercial", TRONCOSO REIGADA, A. (Dir.). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 1.625 a 1.694.

PEÑA LÓPEZ, F., "Capítulo II. De las obligaciones que nacen de culpa o negligencia", BERCOVITZ RODRÍGUEZ-CANO, R., VVAA, *Comentarios al Código Civil, Tomo IX*, Tirant lo Blanch, Valencia, 2013, págs. 12.960 a 13.023.

PÉREZ LUÑO, A.E., *La tercera generación de derechos humanos*, Aranzadi, Cizur Menor (Navarra), 2006.

- *Derechos humanos, estado de derecho y constitución*. 10ª ed., Tecnos, Madrid, 2010.

- "El consentimiento de los menores", TRONCOSO REIGADA, A. (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 473 a 494.

PIÑAR MAÑAS, J.L., "Posibilidad de subcontratación de los servicios", ZABÍA DE LA MATA, J. (Coord.), VVAA, *Protección de datos: comentarios al Reglamento*, Lex Nova, Valladolid, 2008, págs. 237 a 246.

- "Protección de datos: origen, situación actual y retos de futuro", LUCAS MURILLO DE LA CUEVA, P., PIÑAR MAÑAS, J.L., *El derecho a la autodeterminación informativa*, Fundación coloquio jurídico europeo, Madrid, 2009, págs. 81 a 179.

- "Concepto de dato personal", TRONCOSO REIGADA, A. (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 184 a 213.

-*Protección de datos: importante reforma del régimen sancionador*, http://www.abogados.es (fecha consulta: 30.3.2011).

PORCEDDA, M.G., "Law enforcement in the clouds: is the EU data protection legal framework up to the task?", GUTWIRTH, S., LEENES, R., DE HERT, P., POULLET, Y. (Ed.), VVAA, *European Data Protection: in good health?* Springer, Netherlands, 2012, págs. 203 a 232.

POULLET, Y., "Pour une troisième génération de réglementation de protection des données", VERÓNICA, M., PALAZZI, P. (Coord.) VVAA, *Défis du droit à la protection de la vie privée. Challenges of privacy and data protection law*, Bruylant, Bruxelles, Belgique, 2008, págs. 25 a 70.

PRATS ALBENTOSA, L., "Régimen jurídico de los ficheros de solvencia", PRATS ALBENTOSA, L., CUENA CASAS, M. (Coord.), *Préstamo responsable y ficheros de solvencia*, Aranzadi, Cizur Menor (Navarra), 2014, págs. 363 a 406.

PUENTE ESCOBAR, A., "Legitimación para el tratamiento", MARTÍNEZ MARTÍNEZ, R. (Coord.), VVAA, *Protección de datos: comentarios a la LOPD y su reglamento de desarrollo.* Tirant lo Blanch, Valencia, 2009, págs. 37 a 62.

PUYOL MONTERO, J., "Derecho a indemnización", TRONCOSO REIGADA, A. (Dir.). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 1.263 a 1.285.

- *Algunas consideraciones sobre cloud computing, Premio protección de datos personales de investigación 2012*, Agencia Española de Protección de Datos, Agencia Estatal BOE, Madrid, 2013.

QUESADA RODRÍGUEZ, A., *Protección de datos y telecomunicaciones convergentes, Premio protección de datos personales de investigación 2014*, Agencia Española de Protección de Datos, Agencia Estatal BOE, Madrid, 2015.

RALLO LOMBARTE, A., "Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma", *UNED, Revista de derecho político*, nº 85, septiembre-diciembre 2012, págs. 13 a 56.

- *El derecho al olvido en Internet, Google versus España*, Centro de Estudios Políticos y Constitucionales, Madrid, 2014.

REBOLLO DELGADO, L., *Vida privada y protección de datos en la Unión Europea.* Dykinson, Madrid, 2008.

REGLERO CAMPOS, L.F., MEDINA ALCOZ, L., "Capítulo V. El nexo causal. La pérdida de oportunidad. Las causas de exoneración de responsabilidad: culpa de la víctima y fuerza mayor", REGLERO CAMPOS, L.F. (Coord.), VVAA, *Tratado de responsabilidad civil, Tomo I Parte General*, 4ª ed., Aranzadi, Cizur Menor (Navarra), 2008, págs. 721 a 931.

REMOLINA ANGARITA, N., *Recolección internacional de datos personales: un reto del mundo post-internet, Premio protección de datos personales de investigación 2014 Iberoamérica*, Agencia Española de Protección de Datos, Agencia Estatal BOE, Madrid, 2015.

RIASCOS GÓMEZ, L.O., *El derecho a la intimidad, la visión iusinformática y el delito de los datos personales*, Tesis doctoral, Universitat de Lleida, Lleida, 1999.

RODOTÁ, S., "Las lecciones de Wikileaks: nueva transparencia y nueva distribución del poder", PIÑAR MAÑAS, J.L. (Dir.), VVAA, *Transparencia, acceso a la información y protección de datos*, Reus, Madrid, 2014, págs. 9 a 17.

RUBÍ NAVARRETE, J., "El encargado del tratamiento", PALOMAR OLMEDA, A., GONZÁLEZ ESPEJO, P. (Dirs.); ÁLVAREZ RIGAUDIAS, C. (Coord.), VVAA, *Comentario al Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal: (aprobado por RD 1720/2007, de 21 de diciembre)*, Aranzadi, Cizur Menor (Navarra), 2008, págs. 213 a 252.

- "Códigos tipo", MARTÍNEZ MARTÍNEZ, R. (Coord.). *Protección de datos: comentarios a la LOPD y su reglamento de desarrollo.* Tirant lo Blanch, Valencia, 2009, págs. 167 a 199.

RUDA GONZÁLEZ, A., WILSON APONTE, N., "Responsabilidad civil por la inclusión de datos personales en un fichero de solvencia patrimonial", BALCELLS PADULLÉS, J., CERRILLO I MARTÍNEZ, A., PEGUERA POCH, M., PEÑA-LÓPEZ, I., PIFARRÉ DE MONER, M.J., VILASAU SOLANA, M. (Coord.), VVAA, *Internet, Derecho y Política. Una década de transformaciones. Actas del X Congreso Internacional Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona, 3-4 de julio de 2014*, Huygens Editorial, Barcelona, 2014 págs. 259 a 275.

SAN JOSÉ AMAT, C., "Tutela de los derechos", TRONCOSO REIGADA, A. (Dir.). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*. Aranzadi, Cizur Menor (Navarra), 2010, págs. 1.241 a 1.262.

SANCHO VILLA, D., "Ámbito de aplicación territorial", TRONCOSO REIGADA, A. (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 95 a 115.

SANTAMARÍA RAMOS, F. J., *El encargado independiente. Figura clave para un nuevo derecho de protección de datos*, La Ley, Las Rozas (Madrid), 2011.

SERRANO PÉREZ, M.M., *El derecho fundamental a la protección de datos. Derecho español y comparado*, Civitas, Madrid, 2003.

SHACKELFORD, S.J., OTI, E., KERR, J.A., KORZAK, E., KUEHN, A., "Spotlight on cyber V: back to the future of Internet governance", *Georgetown Journal of International Affairs*, June 25, 2015, http://journal.georgetown.edu/back-to-the-future-of-internet-governance/ (fecha consulta: 20.5.2015).

SIBILIA, P., *La intimidad como espectáculo*, Ed. Electrónica, Fondo de Cultura Económica de Argentina, Buenos Aires, Argentina, 2012.

SIMÓN CASTELLANO, P., *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014*, Bosch, Barcelona, 2015.

SOLOVE, D.J., SCHWARTZ, P.M., *Information Privacy Law*, 4ª ed., Wolters Kluwer Law & Business, New York, USA, 2011.

TAVANI, H., "Search engines and Ethics", ZALTA, E. N. (Ed.), *The Stanford Encyclopedia of Philosophy*, Spring 2014 Edition, http://plato.stanford.edu/archives/spr2014/entries/ethics-search/ (fecha consulta: 23.8.2015).

TÉLLEZ AGUILERA, A., *La Protección de datos en la Unión Europea: divergencias normativas y anhelos unificadores*, Edisofer, Madrid, 2002.

TENE, O., "Reforming data protection in Europe and beyond", RALLO LOMBARTE, A., GARCÍA MAHAMUT, R. (Ed.), VVAA, *Hacia un nuevo derecho europeo de protección de datos. Towards a new European data protection regime*, Tirant lo Blanch, Valencia, 2015, págs. 143 a 206.

TRONCOSO REIGADA, A., "La huida de la administración pública hacia el Derecho Privado y la privatización de los servicios públicos: consecuencias en el régimen jurídico de los ficheros de datos personales y en la delimitación del responsable y del encargado del tratamiento." *Anuario de la Facultad de Derecho de Alcalá de Henares*, Nº. 2, 2009, págs. 31 a 110.

- (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010.

-"El principio de calidad de los datos", TRONCOSO REIGADA, A. (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*. Aranzadi, Cizur Menor (Navarra), 2010, págs. 340 a 394.

- "La comunicación de datos personales", TRONCOSO REIGADA, A. (Dir.), VVAA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*. Aranzadi, Cizur Menor (Navarra), 2010, págs. 950 a 1.006.

- *La protección de datos personales. En busca del equilibrio*, Tirant lo Blanch, Valencia, 2010.

- "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *Revista Española de Derecho Europeo*, núm. 43/2012, Aranzadi, págs. 25 a 184.

- "Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales. Parte una" *IDP. Revista de Internet, Derecho y Política*, Número 15, págs. 61 a 75. UOC. http://idp.uoc.edu/ojs/index.php/idp/article/view/n15-troncoso/n15-troncoso-es (fecha consulta: 8.7.2015).

VALERO TORRIJOS, J., FERNÁNDEZ SALMERÓN, M., "Procedimientos administrativos tramitados por la Agencia Española de Protección de Datos", MARTÍNEZ MARTÍNEZ, R. (Coord.). *Protección de datos: comentarios a la LOPD y su reglamento de desarrollo*. Tirant lo Blanch, Valencia, 2009, págs. 266 a 293.

VALERO TORRIJOS, J., "La Administración Pública en la nube. Análisis de las implicaciones jurídicas desde la normativa sobre Administración electrónica", MARTÍNEZ MARTÍNEZ, R. (Ed.), VVAA, *Derecho y cloud computing*, Aranzadi, Cizur Menor (Navarra), 2012, págs. 231 a 253.

VIGURÍ CORDERO, J., "Los mecanismos de certificación (códigos de conducta, sellos y marcas)", RALLO LOMBARTE, A., GARCÍA MAHAMUT, R. (Ed.), VVAA, *Hacia un nuevo derecho europeo de protección de datos. Towards a new European data protection regime*, Tirant lo Blanch, Valencia, 2015, págs. 901 a 957.

VILASAU SOLANA, M., "El caso Google Spain: la afirmación del buscador como responsable del tratamiento y el reconocimiento del derecho al olvido (análisis de la STJUE de 13 de mayo de 2014)", *IDP. Revista de Internet, Derecho y Política*, Número 15, págs. 16 a 32. UOC.

http://journals.uoc.edu/index.php/idp/article/view/n18-vilasau/n18-vilasau-es (fecha consulta: 8.7.2015).

VIZCAÍNO CALDERÓN, M., *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Madrid, 2001.

VULLIET-TAVERNIER, S., "La quantified self: nouvelle forme de partage des données personnelles, nouveaux enjeux?", *IP Innovation & Prospective*, nº 5 juillet 2013.

WACKS, R., *Personal Information, privacy and the law*, Clarendon Press, Oxford, 1989.

WARREN, S.D., BRANDEIS, L.D., "The Right to Privacy", *Harvard Law Review*, Vol. 4 nª5 (Dic.15 1890), págs. 193 a 220.

WEITZNER, D.J., ABELSON, H., BERNERS-LEE, T., FEIGENBAUM, J., HENDLER, J. y SUSSMAN, G.J., "Information Accountability", *Communications of the ACM*, June 2008, Vol. 51, Nº 6, págs. 82 a 87.

WIN, J.K., "Technical standards as data protection regulation", GUTWIRTH, S., POULLET, Y., DE HERT, P., DE TERWANGNE, C., NOUWT, S. (Ed.) VVAA, *Reinventing data protection?* Springer, Nehterlands, 2010, págs. 191 a 207.

DOCUMENTACIÓN

1.- UNIÓN EUROPEA

1.1. Normativa de la Unión Europea

Resolución del Consejo de 7 de mayo de 1985 relativa a una nueva aproximación en materia de armonización y de normalización, DO L 136 de 4.6.1985.

Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO L 281 de 23.11.1995.

Directiva 1999/5/CE del Parlamento Europeo y del Consejo, de 9 de marzo de 1999, sobre equipos radioeléctricos y equipos terminales de telecomunicación y reconocimiento mutuo de su conformidad, DO L 091 de 7.4.1999.

Decisión 1999/468/CE del Consejo, de 28 de junio de 1999, por la que se establecen los procedimientos para el ejercicio de las competencias de ejecución atribuidas a la Comisión, DO L 184 de 17.7.1999.

Decisión del Comité Mixto del EEE nº 83/1999, de 25 de junio de 1999, por la que se modifica el Protocolo 37 y el anexo XI (Servicios de telecomunicaciones) del Acuerdo EEE, DO L 296 de 23.11.2000.

Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), DO L 178 de 17.07.2000.

Decisión de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes publicadas por el Departamento de Comercio de Estados Unidos de América, DO L 215 de 25.8.2000.

Reglamento 45/2001 para la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos DO L 8 de 12.1.2001.

Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE, DO L 181 de 4.7.2001.

Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco), DO L 108 de 24.4.2002.

Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), DO L 201 de 31.7.2002.

Reglamento (CE) n 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información, DO L 77 de 13.3.2004.

Decisión 2004/915/CE de la Comisión, que modifica la Decisión 2001/497/CE respecto a la introducción de unas cláusulas contractuales alternativas para la transferencia de datos personales a países terceros, DO L 385 de 29.12.2004.

Decisión Marco 2008/977/JAI del Consejo de 27 de noviembre de 2008 relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, DO L 350 de 30.12.2008.

Decisión de la Comisión relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo C(2010)593 final, 5.2.2010.

Carta de los Derechos Fundamentales de la Unión Europea, DO C 83 de 30.3.2010 (versión consolidada).

Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, DO L 215/5 de 11.8.2012.

Reglamento (UE) nº 611/2013 de 24 de junio de 2013 relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas, DO 173 de 26.6.2013.

Commission implementing Decision of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy, COM(2015) 102 final, Brussels, 20.1.2015.

1.2. Normativa de los Estados Miembros de la Unión Europea

Ley alemana: *Bundesdatenschutzgesetz* (BDSG). Consultada versión inglesa, *Federal Data Protection Act 14 January 2003*, http://www.gesetze-im-internet.de/englisch_bdsg/federal_data_protection_act.pdf (fecha consulta: 3.8.2015).

Ley austríaca: *Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000* o DSG. BGBI. I nº 165/1999 de 17.8.1999. Consultada versión inglesa, *Federal Act concerning the protection of personal data (DSG 2000)*, http://www.bka.gv.at/datenschutz/dsg2000e.pdf, (fecha consulta: 16.8.2013).

Ley belga: *Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Loi Vie privée* o LVP. http://www.privacycommission.be/sites/privacycommission/files/documents/CONS_loi_vie_privee_08_12_1992.pdf, (fecha consulta: 3.8.2015).

Ley canadiense: *Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c. 5, http://laws-lois.justice.gc.ca/PDF/p-8.6.pdf, (fecha consulta: 2.08.2014).

Ley búlgara: *Law for protection of personal data*, de enero de 2002. Consultada versión inglesa, https://www.cpdp.bg/en/index.php?p=element&aid=373 (fecha consulta: 3.8.2015)

Ley croata: *Personal data protection Act (Official Gazette, Nº. 103/03)*. Consultada versión inglesa,http://www.azop.hr/page.aspx?PageID=79 (fecha consulta: 3.8.2015).

Ley checa: *Personal Data Protection Act, Act No. 101/2000 Coll. of April 4, 2000 on the protection of personal data and on amendments to some Acts*. Consultada versión inglesa, https://www.uoou.cz/en/VismoOnline_ActionScripts/File.ashx?id_org=200156&id_dokumenty=1260 (fecha consulta: 3.8.2015).

Ley chipriota: *The processing of personal data (protection of individuals) law 138(1) 2001*. Consultada versión inglesa, http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/index_en/index_en?opendocument (fecha consulta: 7.10.2013).

Ley danesa: *Act on Processing of Personal Data (Act No. 429 of 31 May 2000*). Consultada versión inglesa, http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/ (fecha consulta: 3.8.2015).

Ley de Liechtenstein: *Data Protection Act of 14 March 2002, Datenschutzgesetz, DSG*. Consultada versión inglesa: http://www.llv.li/pdf-llv-dss-dpa-fl_en_2012-12-07.pdf, (fecha consulta: 30.07.2013).

Ley eslovaca: *Act No. 122/2013 Coll. on personal data protection and on changing and amending of other acts, resulting from amendments and additions executed by the Act No. 84/2014 Coll.*, Consultada versión inglesa publicada, http://www.dataprotection.gov.sk/uoou/sites/default/files/kcfinder/files/Act_122-2013_84-2014_en.pdf (fecha consulta: 3.8.2015).

Ley eslovena: *Personal Data Protection Act (ZVOP-1*) *15 July 2004*. Consultada versión inglesa, https://www.ip-rs.si/fileadmin/user_upload/doc/ZVOP-1_in_ZVOP-1a__English_/Personal_Data_Protection_Act_of_Slovenia_status_2013_final_eng.doc (fecha consulta: 3.8.2015).

Ley estonia: *Personal Data Protection Act 15 February 2007*. Consultada la versión inglesa, http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXX041K1&keel=en&pg=1&ptyyp=RT&tyyp=X&query=isikuandmete+kaitse+seadus (fecha consulta: 3.8.2015).

Ley finlandesa: *Personal Data Act 523/1999*. Consultada versión inglesa, http://www.tietosuoja.fi/uploads/hopxtvf.HTM, (fecha consulta: 11.10.2013).

Ley francesa: *Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée*, http://www.cnil.fr/documentation/textes-fondateurs/loi78-17/, (fecha consulta: 3.8.2015).

Ley griega: *Law 2472/1997 on the protection of individuals with regard to the processing of personal data*. Consultada versión inglesa, http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW%202472-97-NOV2012-EN%20_4_.PDF, (fecha consulta: 20.8.2015).

Ley Países Bajos: *Act of 6 July 2000, Bulletin of Acts, Orders and Decrees 302, containing rules regarding the protection of personal data or Dutch Persona Data Protection Act*. Consultada

versión inglesa, http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.NL (fecha consulta: 20.8.2015).

Ley húngara: *Act CXII of 2011 on the right of informational self-determination and on freedom of information*. Consultada versión inglesa, http://naih.hu/files/Privacy_Act-CXII-of-2011_EN_201310.pdf, (fecha consulta: 20.8.2015).

Ley inglesa: 1998 *Data Protection Act*, 16.7.1998, http://www.legislation.gov.uk/ukpga/1998/29/contents, (fecha consulta: 20.8.2015).

Ley irlandesa: *Data Protection Act 1988 Data Protection Act 1988, Number 25 of 1988, updated to 30 March 2012*, http://www.lawreform.ie/_fileupload/Restatement/First%20Programme%20of%20Restatement/EN_ACT_1988_0025.PDF, (fecha consulta: 20.8.2015).

Ley islandesa: *Act on the protection of privacy as regards the processing of personal data No. 77/2000 of May 10, 2000 or Data Protection Act.* Consultada versión inglesa, http://www.personuvernd.is/information-in-english/greinar/nr/438, (fecha consulta: 20.8.2015).

Ley italiana: *Codice in materia di protezione dei dati personali, Decreto legislativo 30 giugno 2003, n. 196*. Consultadas versiones original e inglesa, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248 y http://194.242.234.211/documents/10160/2012405/DataProtectionCode-2003.pdf, respectivamente, (fecha consulta: 20.8.2015).

Ley letona: *Personal Data Protection Law* 23.3.2000. Consultada versión inglesa, http://www.dvi.gov.lv/eng/legislation/pdp/, (fecha consulta: 10.05.2013).

Ley lituana: *Law on legal protection of personal data No I-1374, 11.6.1996*. Consultada versión inglesa, http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=435305&p_query=&p_tr2=2 (fecha consulta: 20.8.2015).

Ley luxemburguesa: *Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel*. http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002mod_fr.pdf, (fecha consulta: 20.8.2015).

Ley maltesa: *Data Protection Act Chapter 440, 2001*. Consultada versión inglesa, http://idpc.gov.mt/dbfile.aspx/DPA_amended2012.pdf (fecha consulta: 20.8.2015).

Ley noruega: *Act of 14 april 2000 No. 31 relating to the processing of personal data or Personal Data Act.* Consultada versión inglesa, http://app.uio.no/ub/ujur/oversatte-lover/data/lov-20000414-031-eng.pdf (fecha consulta: 20.8.2015).

Ley polaca: *Act of august 29, 1997 on the protection of personal data*. Consultada versión inglesa, http://www.giodo.gov.pl/144/id_art/171/j/en/, (fecha consulta: 20.8.2015).

Ley portuguesa: *Act 67/98 of 26 october on the protection of personal data.* Consultada versión inglesa, http://www.cnpd.pt/english/bin/legislation/Law6798EN.HTM (fecha consulta: 20.8.2015).

Ley rumana: *Law No. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data, amended and completed, 22.10.2001.*

Consultada versión inglesa, http://www.dataprotection.ro/index.jsp?page=legislatie_primara&lang=en (fecha consulta: 20.8.2015).

Ley sueca: *Personal Data Act* 1998:204 http://www.government.se/content/1/c6/01/55/42/b451922d.pdf, (fecha consulta: 30.7.2013).

1.3. Documentos preparatorios y otros

Communication of the Commission of the European Communities to the Council, Community policy on data processing, SEC(73) 4300 final 21.11.1973, http://aei.pitt.edu/6337/1/6337.pdf (fecha consulta: 10.1.2015).

Interim report drawn up on behalf of the Legal Affairs Committee on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing, reporteur: Lord Mansfield, European Communities, European Parliament, Working documents 1974-1975, Document 487/74, 19.2.1975, PE 39, 608/fin./Annex I.

Commission communication on the protection of individuals in relation to the processing of personal data in the Community and Information security, proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data (SYN 287), COM(90) 314 final-SYN 287 and 288, Brussels, 13.9.1990.

Propuesta de Directiva del Consejo relativa a la protección de las personas en lo referente al tratamiento de datos personales, COM(90) 314 final, DO C 277 de 5.11.1990, pág.3.

Outcome of proceedings of Working Party on Economic Questions (Data Protection) on 19 and 20 June 1991, 7284/91, European Communities, The Council, Brussels, 19.7.1991.

Legal Service opinion, Proposal for a Directive on the protection of individuals in relation to the processing of personal data, 8987/91, European Communities, The Council, Brussels, 30.10.1991.

Propuesta modificada de Directiva del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, COM (92) 422 final, DO C 311 de 27.11.1992.

Posición común (CE) nº1/95 adoptada por el Consejo el 20.2.1995 con vistas a la adopción de la Directiva 95/…/CE del Parlamento Europeo y del Consejo, de …, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DOCE C 93, de 13.4.1995.

Recomendación para la segunda lectura del Parlamento Europeo sobre la posición común adoptada por el Consejo con vistas a la adopción de una Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, Comisión de Asuntos Jurídicos y de Derechos de los Ciudadanos, 24.5.1995, PE 212.057/def.

Decisión del Parlamento sobre la posición común del Consejo respecto de una Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO C 166, 3.7.1995.

Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, DO L 024 de 30.1.1998.

Report from the Commission, First report on the implementation of the Data Protection Directive 95/46/EC, COM(2003) 265 final, Brussels,15.5.2003.

Declaración de la Comisión sobre la neutralidad de internet (DO 2009/C 308/2).

Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET), COM(2007) 228 final, Bruselas, 2.5.2007.

Comparative study on different approaches to new privacy challenges, in particular in teh Light of technological developments, Contract _r: JLS/2008/C4/011 – 30-CE-0219363/00-28, Final report, LRDP KANTOR Ltd & Centre for Public Reform, European Commission, Directorate General Justice, Freedom and Security, 20.1.2010.

Comunicación de la Comisión, Europa 2020: Una estrategia para un crecimiento inteligente, sostenible e integrador, COM(2010) 2020 final, Bruselas, 3.3.2010.

KORFF, D., Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Contract _r: JLS/2008/C4/011 – 30-CE-0219363/00-28, Country Studies, A.6-United Kingdom, LRDP KANTOR Ltd & Centre for Public Reform, European Commission, Directorate General Justice, Freedom and Security, June 2010.

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Una agenda digital para Europa, COM(2010) 245 final/2, Bruselas, 26.8.2010.

Comunicación de la Comisión Europea sobre la estrategia para la aplicación efectiva de la Carta de los Derechos Fundamentales por la Unión Europea, COM(2010) 573 final, Bruselas, 19.10.2010.

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, un enfoque global de la protección de los datos personales en la Unión Europea, COM(2010) 609 final, Bruselas, 4.11.2010.

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre "La internet abierta y la neutralidad de la red en Europa", COM(2011) 222 final, Bruselas, 19.4.2011.

Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones — «Un enfoque global de la protección de los datos personales en la Unión Europea» (2011/C 181/01), Bruselas, 22.6.2011

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), draft, Version 56 29.11.2011, http://www.statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf, (fecha consulta: 8.12.2014).

Dictamen del Supervisor Europeo de Protección de Datos sobre la neutralidad de la red, la gestión del tráfico y la protección de la intimidad y los datos personales, DO 2012/C 34/01.

Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), COM(2012)11final 2012/0010 (COD), Bruselas, 25.1.2012.

Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, COM(2012)10 final 2012/0010 (COD), Bruselas, 25.1.2012.

Commission Staff Working Paper, Impact assessment accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. SEC(2012) 72 final, Brussels, 25.1.2012.

Opinion of the European Data Protection Supervisor on the data protection reform package, 7.3.2012.

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Liberar el potencial de la computación en nube en Europa, COM(2012) 529 final, Bruselas, 27.9.2012.

Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", 16.11.2012.

Amendments 165 – 356, Draft opinion Seán Kelly(PE496.562v01-00) on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Proposal for a regulation, (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 20.12.2012.

Enmiendas (2) 602 – 885, Proyecto de informe Jan Philipp Albrecht (PE501.927v04-00) sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) Propuesta de Reglamento, (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 4.3.2013.

Enmiendas (5) 1493 – 1828, Proyecto de informe Jan Philipp Albrecht (PE501.927v04-00) sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) Propuesta de Reglamento, (COM(2012)0011–C7-0025/2012 – 2012/0011(COD)), 6.3.2013.

Enmiendas (6) 1829 – 2090, Proyecto de informe Jan Philipp Albrecht (PE501.927v04-00) sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) Propuesta de Reglamento, (COM(2012)0011–C7-0025/2012 – 2012/0011(COD)), 6.3.2013.

Enmiendas (7) 2091 – 2350, Proyecto de informe Jan Philipp Albrecht (PE501.927v04-00) sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de

las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) Propuesta de Reglamento, (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 6.3.2013.

National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law, Study. Directorate-General for Internal Policies, Policy Department C, Citizen's rights and Constitutional Affairs, European Parliament, PE 493.032, October 2013.

Safe Harbour. Restoring trust in EU-US data flows-Frequently Asked Questions, European Commission MEMO/13/1059, 27.11.2013, Brussels. http://europa.eu/rapid/press-release_MEMO-13-1059_es.htm, (fecha consulta: 2.11.2014).

Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, COM(2013) 847 final, Bruselas, 27.11.2013

Liability for non-compliance with data protection obligations, rough draft presented by M-CH. ROQUES-BONET, L. NETO GALVAO, 2nd meeting of the Commission Expert Group on Cloud computing contracts, 29-30 January 2014. http://ec.europa.eu/justice/contract/files/expert_groups/final_draft_paper_dp_liability_en.pdf (fecha consulta: 12.09.2014).

Note from Presidency to Working Group on Information Exchange and Data Protection (DAPIX) on specific issues of Chapters I-IV of the General Data Protection Regulation-certain aspects of the relationship between controllers and processors. Interinstitutional file: 2012/0011(COD) 5345/14, Council of the EU, Brussels, 15.01.2014.

Note from Presidency to Working Group on Information Exchange and Data Protection (DAPIX). Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)-Article 26. Interinstitutional file: 2012/0011(COD) 5881/14, Council of the EU, Brussels, 31.01.2014.

Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), P7_TA-PROV(2014)0212.

Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos (COM(2012)0010 – C7-0024/2012 – 2012/0010(COD)), P7_TA-PROV(2014)0219.

Resolución del Parlamento Europeo, de 12 de marzo de 2014, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EEUU, los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de justicia y asuntos de interior, P7_TA-PROV(2014)0239.

Factsheet EU-US negotiations on data protection, European Commission, June 2014, http://ec.europa.eu/justice/data-protection/files/factsheets/umbrella_factsheet_en.pdf, (fecha consulta: 2.11.2014).

Commission response to text adopted in European Parliament plenary, SP(2014)455, 10.6.2014.

Recomendación de la Comisión de 10 de octubre de 2014 relativa al modelo de evaluación del impacto sobre la protección de datos para redes inteligentes y para sistemas de contador inteligente, DO L 300 de 18.10.2014.

Privacy and data protection by design-from policy to engineering, European Union Agency for Network and Information Security (ENISA), December 2014.

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, COM(2015) 192 final, Bruselas, 6.5.2015.

Nota de la Presidencia al Consejo sobre Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)-Preparación de un planteamiento general, Expediente interinstitucional: 2012/2011 (COD) 9565/15, Bruselas, 11.6.2015.

Note from General Secretariat of the Council to Delegations on the Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)-Preparation of a general approach, Interinstitutional File: 2021/0011 (COD) 9788/15, Council of the EU, Brussels, 11.6.2015.

Note from General Secretariat of the Council to Permanent Representatives Committee on the Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012, Interinstitutional File: 2013/0309 (COD), Council of the EU, Brussels, 8.7.2015.

Note from Presidency to Working Group on Information Exchange and Data Protection (DAPIX). Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Interinstitutional file: 2012/0011(COD) 10391/15, Council of the EU, Brussels, 8.7.2015.

1.4. Agencia de Derechos Fundamentales de la Unión Europea

Data protection in the European Union: the role of national data protection authorities, strengthening the fundamental rights architecture in the EU II, European Union Agency for Fundamental Rights, Publications Office of the European Union, Luxembourg, 2010. http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf (fecha consulta: 13.8.2014).

Avis FRA – 2/2012 de l'Agence des droits fondamentaux de l'Union européenne concernant le programme de réforme des règles en matière de protection des données à caractère personnel, 1 d'octobre 2012, http://fra.europa.eu/sites/default/files/fra-opinion_2-2012-data-protection_fr.pdf (fecha consulta: 13.8.2014)

Manual de legislación europea en materia de la protección de datos, Oficina de Publicaciones de la Unión Europea, 2014, http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-es.pdf (fecha consulta: 24.6.2015)

1.5. Grupo de trabajo del Artículo 29

Dictamen 1/97 sobre las iniciativas canadienses relativas a la normalización en materia de protección de la intimidad, XV/5023/97 final Corr ES WP 2, 29.5.1997, Grupo de trabajo Artículo 29 sobre la protección de datos.

Documento de trabajo sobre transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la directiva de la UE sobre protección de datos, DG XV D/5025/98, WP12, 24.7.1998, Grupo de trabajo Artículo 29 sobre la protección de datos.

Labor futura en relación con los códigos de conducta: documento de trabajo sobre el procedimiento de examen de los códigos de conducta comunitarios por el Grupo de Trabajo, DG XV D/5004/98 WP 13, 10.9.1998, Grupo de trabajo Artículo 29 sobre la protección de datos.

Dictamen 2/2000 sobre la revisión general de la normativa de telecomunicaciones, 5009/00/ES/final WP 29, 3.2.2000, Grupo operativo sobre internet, Grupo de trabajo Artículo 29 sobre la protección de datos.

Recomendación sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea, 5020/01/ES/Final WP 43, 17.5.2001, Grupo de trabajo Artículo 29 sobre la protección de datos.

Dictamen 10/2001 relativo a la necesidad de un enfoque equilibrado en la lucha contra el terrorismo, 0901/02/ES/Final WP 53, 14.12.2001, Grupo de trabajo Artículo 29 sobre la protección de datos.

Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE, 5035/01/ES/Final WP 56, de 30.5.2002, Grupo de trabajo Artículo 29 sobre la protección de datos.

Dictamen 1/2002 relativo al informe del CEN/ISS sobre la normalización de la protección de la vida privada en Europa, 10761/02/ES/Final WP 57, 30.5.2002, Grupo de trabajo Artículo 29 sobre la protección de datos.

Document de travail: transferts de données personnelles vers des pays tiers: appliclation de l'article 26.2 de la directive de l'UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données, 11639/02/FR WP 74, 3.6.2003, Groupe de travail Article 29 sur la protection des données.

Dictamen 3/2003 relativo al Código de conducta europeo de la FEDMA sobre la utilización de datos personales en la comercialización directa, 10066/03/ES final WP 77, 13.6.2003, Grupo de trabajo Artículo 29 sobre la protección de datos.

Dictamen 10/2004 sobre una mayor armonización de las disposiciones relativas a la información, 11987/04/ES WP 100, 25.11.04, Grupo de trabajo Artículo 29 sobre la protección de datos.

Liste de contrôle type, demande d'approbation de règles d'entreprise contraignantes, 12110/04/FR WP 102, 25.11.2004, Groupe de travail Article 29 sur la protection des données.

Vademecum on notification requirements, version as of 3.7.2006, pursuant to the Working Party document Nº WP106, Article 29 Data Protection Working Party.

Document de travail relatif à une procédure de coopération en vue de l'émission d'avis communs sur le caractère adéquat de la protection offerte par les "règles d'entreprise contraignantes", 05/FR WP 107, 14.4.2005, Groupe de travail Article 29 sur la protection des données.

Document de travail établissant une liste de contrôle type pour les demandes d'approbation des règles d'entreprise contraignantes, 05/FR WP 108, 14.4.2005, Groupe de travail Article 29 sur la protection des données.

Documento de trabajo del Grupo del Artículo 29 relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE, 2093/05/ES WP 114, 25.11.2005, Grupo de trabajo Artículo 29 sobre la protección de datos.

Dictamen 1/2006 relativo a la aplicación de las normas sobre protección de datos de la UE a los sistemas internos de denuncia de irregularidades en los ámbitos de la contabilidad, controles de auditoría internos, cuestiones de auditoría, lucha contra la corrupción y delitos financieros y bancarios, 195/06/ES WP 117, 1.2.2006, Grupo de trabajo Artículo 29 sobre la protección de datos.

Dictamen 8/2006 sobre la revisión del marco regulador de las redes y los servicios de comunicaciones electrónicas, con especial atención a la Directiva sobre la privacidad y las comunicaciones electrónicas, 01611/06/ES WP 126, 26.9.2006, Grupo de trabajo Artículo 29 sobre la protección de datos.

Dictamen 10/2006 sobre el tratamiento de datos personales por parte de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (*Worldwide Interbank Financial Telecommunication*-SWIFT), 01935/06/ES WP 128, 22.11.2006, Grupo de trabajo Artículo 29 sobre la protección de datos.

Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), 00323/07/ES WP 131, 15.2.2007, Grupo de trabajo Artículo 29 sobre la protección de datos.

Recommendation 1/2007 on the standard application for approval of binding corporate rules for the transfert of personal data, WP 133, 10.1.2007, Article 29 Data Protection Working Party.

Dictamen 4/2007 sobre el concepto de datos personales, 012480/07/ES WP 136, 20.6.2007, Grupo de trabajo Artículo 29 sobre la protección de datos.

Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda 00737/ES WP 148, 4.4.2008, Grupo de trabajo Artículo 29 sobre la protección de datos.

Dictamen 2/2008 sobre la revisión de la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas (Directiva sobre privacidad), 00989/08/ES WP 150, 15.5.2008, Grupo de trabajo Artículo 29 sobre la protección de datos.

Document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes, 1271-00/08/FR WP 153, 24.6.2008, Groupe de travail Article 29 sur la protection des données.

Document de travail établissant un cadre pour la structure des règles d'entreprise contraignantes, 1271-00-01/08/FR WP 154, 24.6.2008, Groupe de travail Article 29 sur la protection des données.

Document de travail sur les questions fréquemment posées (FAQ) concernant les règles d'entreprise contraignantes, 1271-04-02/08/FR, WP 155 rév. 04, 24.6.2008, revisé 8.4.2009, Groupe de travail Article 29 sur la protection des données.

Working Document 1/2009 on pre-trial discovery for cross border civil litigation, 00339/09/EN WP 158, 11.02.2009, Article 29 Data Protection Working Party.

Dictamen 5/2009 sobre las redes sociales en línea, 01189/09/ES WP 163, 12.6.2009, Grupo de trabajo Artículo 29 sobre la protección de datos.

El futuro de la privacidad, contribución conjunta a la consulta de la Comisión Europea sobre el marco jurídico del derecho fundamental a la protección de datos de carácter personal, 02356/09/ES WP 168, 1.12.2009, Grupo de trabajo Artículo 29 sobre la protección de datos y Grupo de trabajo Policía y justicia.

Dictamen 1/2010 del Grupo del Artículo 29 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", 00264/10/ES WP 169, 16.2.2010, Grupo de trabajo del Artículo 29 sobre la protección de datos.

Dictamen 3/2010 sobre el principio de responsabilidad, 00062/10/ES GT 173, 13.7.2010, Grupo de trabajo del Artículo 29 sobre la protección de datos.

Dictamen 4/2010 relativo al «Código de conducta europeo de la FEDMA sobre la utilización de datos personales en la comercialización directa», 00065/2010/ES WP 174, 13.7.2010, Grupo de trabajo Artículo 29 sobre la protección de datos.

Dictamen 8/2010 sobre el derecho aplicable, 0836-02/10/ES WP 179, 16.12.2010, Grupo de trabajo Artículo 29 sobre la protección de datos.

Dictamen 15/2011, sobre la definición de consentimiento, 01197/11/ES WP187, 13.7.2011, Grupo de trabajo del Artículo 29 sobre la protección de datos.

Dictamen 01/2012 sobre las propuestas de reforma de la protección de datos, 00530/12/ES WP 191, 23.3.2012, Grupo de trabajo Artículo 29 sobre la protección de datos.

Document de travail 02/2012 établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes pour les sous-traitants, 930/12/FR WP 195, 6.6.2012, Groupe de travail Article 29 sur la protection des données.

Recommendation 1/2012 on the standard application form for approval of binding corporate rules for the transfer of personal data for processing activities, WP 195a, 17.9.2012, Article 29 Data Protection Working Party.

Dictamen 5/2012 sobre la computación en nube, 01037/12/ES WP 196, 1.7.2012, Grupo de trabajo Artículo 29 sobre la protección de datos.

Dictamen 8/2012 por el que se proporciona más información sobre los debates relativos a la reforma de la protección de datos, 01574/12/ES WP 199, 5.10.2012, Grupo de trabajo Artículo 29 sobre la protección de datos.

Working document 01/2013. Input on the proposed implementing acts, 00166/13/EN WP 200, 22.1.2013, Article 29 Data Protection Working Party.

Dictamen 2/2013 sobre las aplicaciones de los dispositivos inteligentes, 00461/13/ES WP 202, 27.2.2013, Grupo de trabajo Artículo 29 sobre la protección de datos.

Opinion 3/2013 on purpose limitation, 00569/13/EN WP 203, 2.04.13, Article 29 Data Protection Working Party.

Explanatory document on the Processor Binding Corporate Rules, 00658/13/EN WP 204 rev.01, 19.4.2013, revised and adopted on 22.5.2015, Article 29 Data Protection Working Party.

Dictamen 2/2014 sobre un documento de referencia para los requisitos en materia de normas corporativas vinculantes presentadas a las autoridades nacionales de protección de datos en la UE y normas de privacidad transfronterizas remitidas a los agentes de rendición de cuentas de dichas normas de la APEC, 538/14/ES, WP 212, 27.2.2014, Grupo de trabajo Artículo 29 sobre la protección de datos.

Working document 1/2014 on draft ad hoc contractual clauses "EU data processor to non-EU sub-processor", 757/14/EN WP 214, 21.03.2014, Article 29 Data Protection Working Party.

Opinion 4/2014 on surveillance of electronic communications for intelligence and national security purposes, 819/14/EN WP 215, 10.04.2014, Article 29 Data Protection Working Party.

Dictamen 5/2014 sobre técnicas de anonimización, 0829/14/ES WP 216, 10.4.2014, Grupo de trabajo Artículo 29 sobre la protección de datos.

Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC, 844/14/EN WP 217, 9.4.2014, Article 29 Data Protection Working Party.

Statement on the role of a risk-based approach in data protection legal frameworks, 14/EN WP 218, 30.5.2014, Article 29 Data Protection Working Party.

Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, 14/EN WP 221, 16.9.2014, Article 29 Data Protection Working Party.

Opinion 8/2014 on the recent developments on the internet of things, 14/EN WP 223, 16.9.2014, Article 29 Data Protection Working Party.

Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12, 14/EN WP 225, 26.11.2014, Article 29 Data Protection Working Party.

Working document setting forth a co-operation procedure for issuing common opinions on "contractual clauses" considered as compliant with the EC model clauses, 14/EN WP 226, 26.11.2014, Article 29 Data Protection Working Party.

1.6. Jurisprudencia del Tribunal de Justicia de la Unión Europea

Sentencia del TJUE de 10 de abril de 1984, *Sabine von Colson et Elisabeth Kamann c. Land Nordrhein-Westfalen*, C-14/83, EU:C:1984:153.

Sentencia del TJUE de 4 de julio de 1985, *Gunter Berkholz*, C-168/84, EU:C:1985:299.

Sentencia del TJUE de 7 de mayo de 1998, *Lease Plan Luxembourg SA*, C-390/96, EU:C:1998:206

Sentencia del TJUE de 20 de mayo de 2003, *Rechnungshof/Österreichischer Rundfunk* y otros C-465/00, C-138/01 y C-139/01, EU:C:2003:294.

Sentencia del TJUE de 6 de noviembre de 2003, *Bodil Lindqvist*, C-101/01, EU:C:2003:596.

Sentencia del TJUE de 30 de mayo de 2006, *Parlamento Europeo/Consejo de la Unión* Europea y Comisión C-317/04 y C-318/04, EU:C:2006:346.

Sentencia del TJUE de 16 de diciembre de 2008, *Heinz Huber*, C-524/06, EU:C:2008:724.

Sentencia del TJUE de 16 de diciembre de 2008, *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy, Satamedia Oy*, C-73/07, EU:C:2008:727.

Sentencia del TJUE de 10 de febrero de 2009, *Irlanda/Parlamento Europeo y Consejo de la Unión Europea*, C-301/06, EU:C:2009:68.

Sentencia del TJUE de 7 de mayo de 2009, *College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer*, C-553/07, EU:C:2009:293.

Sentencia del TJUE de 9 de marzo de 2010, *Comisión Europea c. República federal de Alemania*, C-518/07, EU:C:2010:125.

Sentencia del TJUE de 23 de marzo de 2010, *Google France SARL y Google Inc./Louis Vuitton Malletier SA y otros*, C-236/08 a C-238/08, EU:C:2010:159.

Sentencia del TJUE de 9 de noviembre de 2010, *Vloker und Markus Schecke GbR, Hartmut Eifert*, C-92/09 y C-93/09, EU:C:2010:662.

Sentencia del TJUE de 16 de junio de 2011 *Omejc* c. *Republika Slovenija*, C-536/09, EU:C:2011:398.

Sentencia del TJUE de 22 de septiembre de 2011, *Interflora Inc* y *Interflora British Unit/ Mark&Spencer plc* y *Flowers Direct Online Ltd*, C-323/09, EU:C:2011:604.

Sentencia del TJUE de 24 de noviembre de 2011, *ASNEF, FECEMD/Administración del Estado*, C-468/10 y C-469/10, EU:C:2011:777.

Sentencia del TJUE de 24 de noviembre de 2011, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, EU:C:2011:771.

Sentencia del TJUE de 16 de febrero de 2012, *SABAM/Netlog NV*, C-360/10, EU:C:2012:85.

Sentencia del TJUE de 22 de noviembre de 2012 *Probst*, C-119/12, EU:C:2012:748

Sentencia del TJUE de 30 de mayo de 2013, *Worten*, C-342/12, EU:C:2013:355.

Conclusiones del Abogado General Niilo Jääskinen de 25 de junio de 2013 en el asunto *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2013:424.

Sentencia del TJUE de 17 de octubre de 2013, *Schwarz*, C-291/12, EU:C:2013:670.

Sentencia del TJUE de 7 de noviembre de 2013, *IPI*, C-473/12, EU:C:2013:715.

Sentencia del TJUE de 12 de diciembre de 2013, *X*, C-486/12, EU:C:2013:836.

Sentencia del TJUE de 8 de abril de 2014, *Digital Rights Ireland* y *Seitlinger* y otros, C-293/12 y C-594/12, EU:C:2014:238.

Sentencia del TJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, EU:C:2014:317.

Sentencia del TJUE de 17 de julio de 2014 *YS*, C-141/12 y C/372/12, EU:C:2014:2081.

Petición de decisión prejudicial planteada por la *High Court of Ireland* (Irlanda) el 25 de julio de 2014, *Maximillian Schrems/Data Protection Commissioner*, C-362/14, DO C 351 de 6.10.2014.

Sentencia del TJUE de 4 de septiembre de 2014 *Vnuk*, C-162/13, EU:C:2014:2146.

Sentencia del TJUE de 11 de diciembre de 2014 *Rynes*, C-212/13, EU:C:2014:2428

1.7. Autoridades de control

The guide to data protection, Information Commissioner's Office (ICO). http://www.ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Practical_application/the_guide_to_data_protection.pdf, (fecha consulta: 24.8.13).

Privacy notices code of practice, Information Commissioner's Office (ICO), http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_notices_cop_final.pdf, (fecha de consulta: 24.8.13).

Data Protection Act 1998 Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998, ICO, The Stationery Office, 2012, London. http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ico_guidance_on_monetary_penalties.pdf (fecha consulta: 14.8.2014).

Conducting privacy impact assessments code of practice, Information Commissioner's Office (ICO), 25.02.2014. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf, (fecha consulta: 27.12.2014).

Délibération no 2011-249 du 8 septembre 2011 portant modification de l'article 69 du règlement, intérieur de la Commission nationale de l'informatique et des libertés et insérant un chapitre IV bis intitulé « Procédure de labellisation », Commission nationale de l'informatique et des libertés, Journal Officiel de la République Française, 22 septembre 2011: http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=20110922&numTexte=81&pageDebut=&pageFin=, (fecha consulta: 12.08.2014).

Working paper on cloud computing-Privacy and data protection issues, "Sopot Memorandum", International Working Group on Data Protection in Telecommunications, Sopot (Poland), 24.4.2012.

Délibération no 2011-316 du 6 octobre 2011 portant adoption d'un référentiel pour la délivrance de labels en matière de procédure d'audit tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, Commission nationale de l'informatique et des libertés, Journal Officiel de la République Française, 3 novembre 2011, http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=20111103&numTexte=63&pageDebut=&pageFin=, (fecha consulta: 12.8.2014).

Délibération no 2011-315 du 6 octobre 2011 portant adoption d'un référentiel pour la délivrance de labels en matière de formation tendant à la protection des personnes à l'égard du traitement des données à caractère personnel Commission nationale de l'informatique et des libertés, Journal Officiel de la République Française, 3 novembre 2011, http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=20111103&numTexte=62&pageDebut=&pageFin= (fecha consulta: 12.8.2014).

Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing, CNIL, 25.06.2012. http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf, (fecha consulta: 23.9.2014).

Recommandation nº 04/2015 du 13 mai 2015, Comission de la protection de la vie privée (Autoridad belga de protección de datos). http://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_04_2015.pdf (fecha consulta: 8.7.2015)

2. CONSEJO DE EUROPA

2.1. Normativa

Convenio de Roma, de 4 de noviembre de 1950, para la Protección de los Derechos Humanos y de las Libertades Fundamentales, firmado por España el 24 de noviembre de 1977 y ratificado el 4 de octubre de 1979 (BOE núm. 243 de 10.10.1985)

Convenio Europeo de Derechos Humanos, Tribunal europeo de Derechos Humanos, Consejo de Europa, Estrasburgo, versión española no oficial, http://www.echr.coe.int/Documents/Convention_SPA.pdf (fecha consulta: 21.6.2015).

Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (BOE núm. 274 de 15.11.1985).

Resolución (73) 22, de 26 de septiembre de 1973 del Comité de Ministros del Consejo de Europa, relativa a la protección de la vida privada de las personas físicas con respecto a los bancos de datos electrónicos en el sector privado.

Resolución (74) 29, de 20 de septiembre de 1974 del Comité de Ministros del Consejo de Europa, referente a la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector público.

Recomendación CM/Rec(2014)6 del Comité de Ministros del Consejo de Europa de 16 de abril de 2014.

2.2. Documentos preparatorios y otros

Observations by the French authorities on the draft Resolution, Sub-Committee of the European Committee on Legal Co-Operation charged with examining a draft resolution on the protection of privacy vis-a-vis Electronic data Banks in the private sector, CCJ/SC. Prot. Priv. (73)2, Strasbourg, 28 February 1973.

Observations by the Danish authorities, Sub-Committee of the European Committee on Legal Co-Operation charged with examining a draft resolution on the protection of privacy vis-a-vis

Electronic data Banks in the private sector, CCJ/SC. Prot. Priv. (73)3, Strasbourg, 15 March 1973.

Draft Convention for the protection of individuals with regard to automated data files prepared by the Secretariat following the meeting of Working Party No. 1 of the Committee of Experts on Data Protection (CJ-PD-GT1) held in Strasbourg from 16 to 18 January 1979, Council of Europe, CJ-PD-GT1 (79)1, Strasbourg, 19 January 1979.

Commentaires du Secrétariat au projet révisé de Convention pour la protection des personnes à l'égard des fichiers automatisés, Comité d'experts sur la protection des données, Conseil de l'Europe, CJ-PD-GT1 (79)2, Strasbourg, 22 Janvier 1979.

Draft Convention for the protection of individuals with regard to automated data files (CJ-PD-GTI (79)1), Committee of experts on data protection, Working Group No. 1, Comments of the Spanish experts, CJ-PD-GT1 (79)5, Strasbourg, 22 March 1979.

Rapport abrégé de la 23e réunion (Strasbourg 14-16 mars 2007), CM/Inf(2007)24 Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE Nº 108)-(T-PD), Strasbourg, 4 Mai 2007.

Data protection compilation of Council of Europe texts, Directorate General of Human Rights and Legal Affairs, Council of Europe, Strasbourg, November 2010.

Draft explanatory report of the modernised version of Convention 108, CASHDATA(2014)06, Council of Europe Ad hoc Committee on data protection (CAHDATA), Council of Europe, Strasbourg, 23 November 2014.

Abridged report of the 3rd and final meeting (Strasbourg, 1-3 December 2014), CM(2015)40, Ad hoc Committe on Data Protection (CAHDATA), Council of Europe, Strasbourg, 3 March 2015.

Draft abridged report of the 32nd Plenary meeting (Strasbourg, 1-3 July), T-PD(2015)RAP32Abr_en, Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) (T-PD), Council of Europe, Strasbourg, 2 July 2015.

2.3. Jurisprudencia del Tribunal Europeo de Derechos Humanos

Sentencia del TEDH de 17 de octubre de 2008, *I v. Finland*.

Sentencia del TEDH de 4 de diciembre de 2008, *S. and Marper v. The United Kingdom*.

Sentencia del TEDH de 2 de marzo de 2009, *K.U. v. Finland*.

Sentencia del TEDH de 18 de marzo de 2013, *Yildirim c. Turquía*.

Sentencia del TEDH de 27 de agosto de 2014, *La Flor Cabrera c. Espagne*.

3. ORGANIZACIÓN DE NACIONES UNIDAS (ONU)

Declaración Universal de Derechos Humanos aprobada en 1948 aprobada por Resolución de la Asamblea General de la ONU 217 A(III) del 10 de diciembre de 1948.

Pacto Internacional de Derechos Civiles y Políticos aprobado por la Asamblea General de la ONU en su resolución 2200 A (XXI), de 16 de diciembre de 1966.

Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales aprobados por la Resolución 45/95 de la Asamblea General de Naciones Unidas, de 14 de diciembre de 1990.

Informe del Secretario General de la Asamblea General de la ONU A/44/606, de 24 de octubre de 1989, sobre los Principios rectores para la reglamentación de los ficheros computadorizados de datos personales.

Proyecto de resolución presentado por Alemania y Brasil a la Asamblea General de Naciones Unidas sobre "El derecho a la privacidad en la era digital" el 1 de noviembre de 2013, Sexagésimo octavo período de sesiones, Tercera Comisión, Tema 69b) del programa, Promoción y protección de los derechos humanos: cuestiones de derechos humanos, incluidos otros medios de mejorar el goce efectivo de los derechos humanos y las libertades fundamentales, A/C.3/68/L.45.

4. ORGANIZACIÓN DE COOPERACIÓN Y DESARROLLO ECONÓMICO (OCDE)

Guía de la OCDE relativa a la protección de la privacidad y de las transferencias de datos personales aprobada por resolución del Consejo de 23 de septiembre de 1980. *OECD Guidelines on the protection of privacy and transborder flows of personal data.* http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (fecha consulta: 21.7.2014).

Recommendation of the Council concerning Guidelines governing the protection of privacy and transborder flows of personal data (2013), C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79. http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (fecha consulta: 21.7.2014).

"*Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines*", *OECD Digital Economy Papers, No. 229, OECD Publishing*. http://dx.doi.org/10.1787/5k3xz5zmj2mx-en (fecha consulta: 8.8.2014).

5. COOPERACIÓN ECONÓMICA ASIA-PACÍFICO (APEC)

Asia-Pacific Economic Cooperation Privacy Framework, APEC#205-SO-01.2, APEC Electronic Commerce Steering Group (ECSG), 2005. http://publications.apec.org/publication-detail.php?pub_id=390 (fecha consulta: 11.8.2014).

Guidebook on APEC privacy and trustmark, APEC#212-CT-03.2, Electronic Commerce Steering Group, APEC, November 2012, http://publications.apec.org/publication-detail.php?pub_id=1345 (fecha consulta: 11.8.2014).

6. ESPAÑA

6.1. Normativa

Instrumento de ratificación del Convenio relativo a la obtención de pruebas en el extranjero en materia civil o mercantil, hecho en La Haya el 18 de marzo de 1970 (BOE núm. 203 de 25.8.1987)

Ley Orgánica 2/1979, de 3 de octubre, del Tribunal Constitucional (BOE núm. 239 de 5.10.1979).

Ley 7/1985, de 2 de abril, reguladora de las bases de régimen local (BOE núm. 80 de 3.4.1985)

Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. (BOE núm. 285 de 27.11.1992).

Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos (BOE núm. 106 de 4.5.1993).

Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contencioso-administrativa (BOE núm. 167 de 14.7.1998).

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (BOE núm. 166 de 12.7.2002).

Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (BOE núm. 274 de 15.11.2002)

Decreto 48/2003, de 20 de febrero por el que se aprueba el Estatuto de la *Agència Catalana de Protecció de Dades* (DOGC núm. 3835 de 4.3.2003).

Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos (BOPV núm. 44 de 4.3.2004 y BOE núm. 279 de 19.11.2011).

Real Decreto 1163/2005, de 30 de septiembre, por el que se regula el distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico, así como los requisitos y el procedimiento de concesión. (BOE núm. 241 8.10.2005).

Decreto 309/2005, de 18 de octubre, por el que se aprueba el Estatuto de la Agencia Vasca de Protección de Datos (BOPV núm. 213 de 9.11.2005).

Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (BOE núm. 150 de 23.6.2007)..

Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, (BOE núm. 25 de 29.01.2010, Sec. I Pág. 8089).

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (BOE núm. 25 de 29.01.2010, Sec. I Pág. 8139).

Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos (DOGC núm. 5731 de 8.10.2010).

Ley 37/2011, de 10 de octubre, de medidas de agilización procesal (BOE de 11.10.2011).

Real Decreto 869/2013, de 8 de noviembre, por el que se modifica el Real Decreto 1553/2005, de 23 de diciembre, que regula la expedición del documento nacional de identidad y sus certificados de firma electrónica (BOE núm. 281 de 23.11.2013).

Ley 29/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (BOE núm. 295 de 10.12.2013).

Ley 5/2014, de 4 de abril, de seguridad privada (BOE núm. 83 de 5.4.2014).

Ley 19/2014, del 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno (DOGC núm. 6780 de 31.12.2014).

6.2. Documentos preparatorios y otros

Debate de totalidad del Proyecto de Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal. "Boletín Oficial de las Cortes Generales", Serie A, número 59.1, de 24 de julio de 1991 (número de expediente 121/000059). Cortes Generales, Diario de Sesiones del Congreso de los Diputados, Pleno y diputación permanente, IV Legislatura, núm. 145, sesión plenaria del 28 de noviembre de 1991.

Dictamen de la Comisión Constitucional a la vista del informe elaborado por la Ponencia, sobre el Proyecto de Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal (BOCG, Serie A, nº 59-1, de 24-7-91)(número de expediente 121/000059) (continuación). Cortes Generales, Diario de sesiones del Congreso de los Diputados, Comisiones, Constitucional, IV Legislatura, nº 425, sesión de 8 de abril de 1992.

Enmiendas al Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (núm. 121/000135), BOCG, Congreso de los Diputados, VI Legislatura, Serie A: Proyectos de Ley, núm. 135-7, presentación de enmiendas, 4 de noviembre de 1998.

Informe de la ponencia sobre el Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (núm. 121/000135), BOCG, Congreso de los Diputados, VI Legislatura, Serie A: Proyectos de Ley, núm. 135-9, presentación de enmiendas, 14 de septiembre de 1999.

Dictamen de la Comisión Constitucional a la vista del informe elaborado por la Ponencia, sobre el Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (núm. 121/000135), Diario de Sesiones del Congreso de los Diputados, VI Legislatura, Comisión Constitucional, Sesión núm. 24 de 15 de septiembre de 1999, núm. 744.

Enmiendas del Senado al Proyecto de Ley Orgánica de Protección de Datos, BOCG, Congreso de los Diputados, serie A, número 135-1, de 31 de agosto de 1998 (Número de expediente 121/000135), *Diario de Sesiones del Congreso de los Diputados*, Pleno y diputación permanente, VI Legislatura, núm. 277, Sesión plenaria núm. 267 celebrada el 25 de noviembre de 1999, págs. 14931-14932.

Declaración del Pleno del Tribunal Constitucional 1/2004, de 13 de diciembre de 2004. Requerimiento 6603-2004. Formulado por el Gobierno de la Nación, acerca de la constitucionalidad de los artículos I-6, II-111 y II-112 del Tratado por el que se establece una Constitución para Europa, firmado en Roma el 29 de octubre de 2004. BOE núm. 3 Suplemento, de 4.1.2005, pág. 5.

Intervención del Director de la AEPD don José Luis Rodríguez Álvarez. Cortes Generales, Diario de Sesiones del Congreso de los Diputados, Comisiones Constitucional, X Legislatura, núm. 205, sesión del 7 de noviembre de 2012.

Aprobación por la Comisión de Interior del Informe de la Subcomisión de estudio sobre las redes sociales, BOCG, Congreso de los Diputados, X Legislatura, serie D: general, número 643-1, de 9 de abril de 2015.

6.3. Jurisprudencia

6.3.1. Tribunal Constitucional

STC 76/1990 de 26 de abril de 1990, recurso de inconstitucionalidad y cuestiones de inconstitucionalidad relativos a determinados preceptos de la Ley 10/1985, de 26 de abril, de modificación parcial de la Ley General Tributaria.

STC 254/1993, de 20 de julio de 1993, recurso de amparo contra denegación presunta por parte del Gobernador Civil de Guipúzcoa y del Ministro del Interior de solicitud de información de los datos de carácter personal existentes en ficheros automatizados de la Administración del Estado, confirmada en la vía contencioso-administrativa. Vulneración del derecho a la intimidad personal. Voto particular.

STC 11/1998, de 13 de enero de 1998, recurso de amparo contra sentencia de la sala de lo social del TSJ de Madrid dictada en procedimiento de tutela de derechos fundamentales.

STC 290/2000, de 30 de noviembre de 2000, recursos de inconstitucionalidad contra la Ley Orgánica 5/1992, de 29 de octubre de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

STC 292/2000, de 30 de noviembre de 2000, recurso de inconstitucionalidad contra la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

ATC 57/2007, de 26 de febrero de 2007, que inadmite recurso de amparo 4243-2003 promovido contra sentencia del Tribunal Superior de Justicia de Cantabria, que desestimó recurso contencioso-administrativo por el procedimiento especial para la tutela de los derechos fundamentales contra la actuación material consistente en la implantación de un sistema de control de permanencia del personal al servicio de dicha Administración mediante un equipo digital.

STC 160/2008, de 2 de diciembre, recurso de amparo promovido contra sentencia de la Audiencia Nacional que desestimó la demanda sobre responsabilidad patrimonial de la Administración del Estado del recurrente. Vulneración de los derechos de igualdad en la aplicación de la ley y a la tutela judicial efectiva, sentencia que cambia de criterio respecto al aplicado a otros perjudicados por el mismo accidente de tráfico sin justificación.

ATC 20/2011, de 28 de febrero de 2011, que inadmite a trámite el recurso de amparo 9929-2008, promovido por la Agencia española de protección de datos, en contencioso sobre cancelación de datos obrantes en los libros bautismales. Voto particular.

STC 96/2012, de 7 de mayo de 2012, recurso de amparo promovido por la entidad BBVA en relación con las diligencias preliminares de juicio acordadas por un Juzgado de Primera Instancia en las que se ordena la entrega a una asociación de usuarios de la relación de personas que hubieran contratado determinados productos financieros.

STC 219/2012, de 26 de noviembre de 2012, recurso de amparo promovido en relación con unas diligencias preliminares de juicio acordadas por un Juzgado de Primera Instancia en las que se rechaza la personación de quienes se vieron afectados por la decisión judicial de ordenar la entrega a una asociación de usuarios de la relación de personas que hubieran contratado determinados productos financieros.

STC 29/2013, de 11 de febrero de 2013, recurso de amparo respecto a sentencias del Tribunal de Justicia de Andalucía y de un Juzgado de lo Social de Sevilla parcialmente estimatorias de la impugnación del recurrente de la sanción disciplinaria impuesta por la Universidad de Sevilla.

Vulneración del derecho a la protección de datos de carácter personal por utilización de imágenes captadas por las cámaras de videovigilancia instaladas en el recinto universitario para una finalidad, la supervisión laboral, de la que no se informó al trabajador. Voto particular.

6.3.2. Tribunal Supremo

STS 12 de diciembre de 1995 (Sala 3ª) (ROJ: STS 6316/1995)
STS de 5 de junio de 2004 (Sala 3ª) (ROJ: STS 3896/2004)
STS de 18 de junio de 2004 (Sala 3ª) (ROJ: STS 4258/2004)
STS de 28 de diciembre de 2004 (Sala 3ª) (ROJ STS 8494/2004)
STS de 28 de febrero de 2005 (Sala 3ª) (ROJ: STS 1234/2005)
STS 18 de marzo de 2005 (Sala 3ª) (ROJ: STS 1730/2005)
STS de 26 de abril de 2005 (Sala 3ª) (ROJ: STS 2570/2005)
STS de 18 de julio de 2006 (Sala 3ª) (ROJ: STS 4510/2006)
STS de 23 de enero de 2007 (Sala 3ª) (ROJ: STS 224/2007)
STS de 19 de septiembre de 2008 (Sala 3ª) (ROJ: STS 4646/2008)
STS de 4 de mayo de 2009 (Sala 3ª) (ROJ: STS 2651/2009)
STS de 30 de diciembre de 2009 (Sala 2ª) (ROJ: STS 8457/2009)
STS de 29 de junio de 2010 (Sala 3ª) (ROJ: STS 3674/2010)
STS de 15 de julio de 2010 (Sala 3ª) (ROJ: STS 4050/2010)
STS de 15 de julio de 2010 (Sala 3ª) (ROJ: STS 4057/2010)
STS de 17 de septiembre de 2010 (Sala 3ª) (ROJ: STS 4940/2010)
STS de 9 de diciembre de 2010 (Sala 2ª) (ROJ: STS 7064/2010)
STS de 30 de marzo de 2011 (Sala 1ª) (ROJ: STS 2227/2011)
STS de 10 de junio de 2011 (Sala 3ª) (ROJ: STS 3668/2011)
STS de 2 de diciembre de 2011 (Sala 3ª) (ROJ: STS 8497/2011)
STS de 8 de febrero de 2012 (Sala 3ª) (ROJ: STS 429/2012)
STS de 3 de abril de 2012 (Sala 1ª) (ROJ: STS 3942/2012)
STS de 9 de abril de 2012 (Sala 1ª) (ROJ: STS 2638/2012)
STS de 13 de noviembre de 2012 (Sala 3ª) (ROJ: STS 7404/2012)
STS de 20 de marzo de 2013 (Sala 1ª) (ROJ: STS 2249/2013)
STS de 15 de enero de 2014 (Sala 1ª) (ROJ: STS 69/2014)
STS de 22 de enero de 2014 (Sala 1ª) (ROJ: STS 355/2014)
STS de 25 de marzo de 2014 (Sala 3ª) (ROJ:STS 1203/2014)
STS de 13 de mayo de 2014 (Sala 4ª) (ROJ:STS 2618/2014)
STS de 21 de mayo de 2014 (Sala 1ª) (ROJ: STS 267/2014)
STS de 9 de junio de 2014 (Sala 3ª) (ROJ: STS 2365/2014)
STS de 17 de junio de 2014 (Sala 2ª) (ROJ: STS 3545/2014)
STS de 17 de septiembre de 2014 (Sala 1ª) (ROJ: STS 3524/2014)

6.3.3. Audiencia Nacional

SAN de 4 de abril de 2002 (Sala de lo contencioso-administrativo) (ROJ: SAN 2028/2002)
SAN de 13 de septiembre de 2002 (Sala de lo contencioso-administrativo) (ROJ: SAN 4954/2002)
SAN de 20 de septiembre de 2002 (Sala de lo contencioso-administrativo) (ROJ: SAN 5137/2002)
SAN de 15 de noviembre de 2002 (Sala de lo contencioso-administrativo) (ROJ: SAN 6324/2002)
SAN de 16 de octubre de 2003 (Sala de lo contencioso-administrativo) (ROJ: SAN 1936/2003)
SAN de 11 de febrero de 2004 (Sala de lo contencioso-administrativo) (ROJ: SAN 845/2004)
SAN de 17 de marzo de 2004 (Sala de lo contencioso-administrativo) (ROJ: SAN 1914/2004)
SAN de 9 de junio de 2004 (Sala de lo contencioso-administrativo) (ROJ: SAN 4112/2004)
SAN de 13 de abril de 2005 (Sala de lo contencioso-administrativo) (ROJ: SAN 6741/2005)
SAN de 13 de abril de 2005 (Sala de lo contencioso-administrativo) (ROJ: SAN 6766/2005)

SAN de 21 de septiembre de 2005 (Sala de lo contencioso-administrativo) (ROJ: SAN 4494/2005)
SAN de 16 de febrero de 2006 (Sala de lo contencioso-administrativo) (ROJ: SAN 822/2006)
SAN de 25 de mayo de 2006 (Sala de lo contencioso-administrativo) (ROJ: SAN 2284/2006)
SAN de 22 de junio de 2006 (Sala de lo contencioso-administrativo) (ROJ: SAN 3072/2006)
SAN de 5 de mayo de 2008 (Sala de lo contencioso-administrativo) (ROJ: SAN 523/2008)
SAN de 4 de junio de 2008 (Sala de lo contencioso-administrativo) (ROJ: SAN 2243/2008)
SAN de 23 de septiembre de 2008 (Sala de lo contencioso-administrativo) (ROJ: SAN 3728/2008)
SAN de 7 de mayo de 2009 (Sala de lo contencioso-administrativo) (ROJ: SAN 2285/2009)
SAN de 16 de julio de 2009 (Sala de lo contencioso-administrativo) (ROJ: SAN 3789/2009)
SAN de 16 de julio de 2009 (Sala de lo contencioso-administrativo) (ROJ: SAN 3804/2009)
SAN de 21 de enero de 2010 (Sala de lo contencioso-administrativo) (ROJ: SAN 438/2010)
SAN de 22 de julio de 2010 (Sala de lo contencioso-administrativo) (ROJ: SAN 3604/2010)
SAN de 6 de mayo de 2011(Sala de lo contencioso-administrativo) (ROJ: SAN 2198/2011)
SAN de 9 de junio de 2011 (Sala de lo contencioso-administrativo) (ROJ: SAN 2846/2011)
SAN de 20 de octubre de 2011(Sala de lo contencioso-administrativo) (ROJ: SAN 5251/2011)
AAN de 27 de febrero de 2012 (Sala de lo contencioso-administrativo) (ROJ: AAN 19A/2012)
SAN de 11 de abril de 2012 (Sala de lo contencioso-administrativo) (ROJ: SAN 1702/2012)
SAN de 31 de mayo de 2012 (Sala de lo contencioso-administrativo) (ROJ: SAN 2747/2012)
SAN de 4 de marzo de 2013 (Sala de lo contencioso-administrativo) (ROJ: SAN 971/2013)
SAN de 17 de mayo de 2013 (Sala de lo contencioso-administrativo) (ROJ: SAN 2172/2013)
SAN de 29 de diciembre de 2014 (Sala de lo contencioso-administrativo) (ROJ: SAN 4899/2014)

6.3.4. Audiencias Provinciales

SAP Valladolid de 14 de julio de 1998 (Sección 2) (ROJ: SAP VA 1374/1998)
SAP Segovia de 25 de abril de 2002 (Sección 1) (ROJ: SAP SG 168/2002)
SAP Madrid de 31 de marzo de 2006 (Sección 11) (ROJ: SAP M 4152/2006)
SAP Cádiz de 27 de octubre de 2006 (Sección 8) (ROJ: SAP CA 2463/2006)
SAP Islas Baleares de 30 de junio de 2006 (Sección 4) (ROJ: SAP IB 1569/2006)
SAP Madrid de 25 de enero de 2012 (Sección 10) (ROJ: SAP M 1922/2012)
SAP Barcelona de 17 de julio de 2014 (Sección 16) (ROJ: SAP B 8246/2014)

6.4. Autoridades de control

6.4.1. Agencia Española de Protección de Datos

a. Instrucciones

Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, BOE núm. 296, 12.12.06, págs. 43458-43460.

b. Informes

Informes de 1999 sin referencia.
Informe de 2002 sin referencia.
Informe 0060/2004
Informe 0582/2004
Informe 0167/2005
Informe 0365/2006
Informe 0128/2007
Informe 0042/2008
Informe 0078/2008

Informe 0106/2008
Informe 0200/2008
Informe 0234/2008
Informe 0457/2008
Informe 0541/2008
Informe 0569/2008
Informe 0279/2009
Informe 0295/2009
Informe 0488/2009
Informe 0573/2009
Informe 0636/2009
Informe 0645/2009
Informe 0654/2009
Informe 0016/2010
Informe 0037/2010
Informe 0039/2010
Informe 0267/2010
Informe 0427/2010
Informe 0523/2010
Informe 0352/2011
Informe 0241/2011
Informe 0112/2012
Informe 0333/2012

c. Resoluciones

Resolución R/02340/2009 de la AEPD, de 20 de noviembre de 2009, PS/00381/2009
Resolución R/00347/2010 de la AEPD, de 22 de febrero de 2010, PS/304/2009
Resolución 1680/2010 de la AEPD, de 30 de julio de 2010, TD/650/2010
Resolución TI/00126/2012 de la AEPD, de 16 de octubre de 2012
Resolución R/02892/2013 de la AEPD, de 18 de diciembre de 2013, PS/00345/2013.
Resolución TI/00032/2014 de la AEPD, de 9 de mayo de 2014

d. Otros

Memoria de la Agencia Española de Protección de Datos de 1994
Memoria de la Agencia Española de Protección de Datos de 1995
Memoria de la Agencia Española de Protección de Datos de 2011
Memoria de la Agencia Española de Protección de Datos de 2013
Memoria de la Agencia Española de Protección de Datos de 2014

Recomendaciones referentes al plan de inspección de oficio a las empresas participantes en la elaboración de los censos de población y viviendas del año 2001 de 17.7.2003.

FAQ's 1ª sesión abierta de la AEPD de 22 de abril de 2008, Creación e inscripción de ficheros, Transferencias internacionales, Códigos tipo, Medidas de seguridad, Inspección y potestad sancionadora, http://www.agpd.es/portalwebAGPD/jornadas/1_sesion_abierta/common/faqs_bloque_2.pdf (fecha consulta: 14.2.2015).

Nota de prensa de la AEPD de 30.9.2008: http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2008/notas_prensa/common/sept/np_080930_sentencia_TS.pdf, (fecha consulta: 10.2.2015).

Ponencia de la Jornada Abierta, celebrada el 27 de abril de 2012, sobre Cloud computing: Sujetos que intervienen, Ley aplicable, Garantías, J. RUBÍ NAVARRETE, AEPD, pág. 9 http://www.agpd.es/portalwebAGPD/jornadas/4_sesion_abierta_2011/common/CLOUD_COMPUTING.pdf (fecha consulta: 23.9.2014)

Guía para clientes que contraten servicios de Cloud Computing, Agencia Española de Protección de Datos, 2013, http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf, (fecha consulta: 23.9.2014).

Orientaciones para prestadores de servicios de Cloud Computing, Agencia Española de Protección de Datos, 2013, http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/ORIENTACIONES_Cloud.pdf, (fecha consulta: 23.9.2014).

Guía para una Evaluación de Impacto en la protección de datos personales, publicada el 29 de octubre de 2014. Agencia Española de Protección de Datos. http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf, (fecha consulta: 27.12.2014).

6.4.2. Autoritat Catalana de Protecció de Dades

Instrucción 1/2009, de 10 de febrero, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia, DOGC, núm. 5322, 19.2.2009, págs. 13258-13272.

Recomendación 1/2010 de la Agència Catalana de Protecció de Dades, sobre el encargado de tratamiento en la prestación de servicios por cuenta de entidades del sector público de Cataluña.

Recomendación 1/2011 de la Autoritat Catalana de Protecció de Dades sobre la creación, modificación y supresión de ficheros de datos de carácter personal de titularidad pública

Guía básica de protección de datos para los colegios profesionales, Generalitat de Catalunya, Autoritat Catalana de Protecció de Dades, 2014

Dictamen CNS-10/2006 de la Autoritat Catalana de Protecció de Dades
Dictamen CNS-13/2007 de la Autoritat Catalana de Protecció de Dades
Dictamen CNS-28/2013 de la Autoritat Catalana de Protecció de Dades
Dictamen CNS-57/2013 de la Autoritat Catalana de Protecció de Dades
Dictamen CNS-27/2014 de la Autoritat Catalana de Protecció de Dades

7. ESTADOS UNIDOS

Records computers and the rights of citizens, report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education & Welfare, July 1973. http://www.justice.gov/sites/default/files/opcl/docs/rec-com-rights.pdf (fecha consulta: 30.07.2014).

Overview of the Privacy Act of 1974, Department of Justice's Office of Privacy and Civil Liberties, http://www.justice.gov/opcl/1974privacyact-overview.htmp (fecha consulta: 20/01/2013).

The fair information practice principles: framework for privacy policy at the Department of Homeland Security, Privacy policy guidance memorandum 2008-01, The Privacy Office, U.S. Department of Homeland Security, 29.12.2008,

http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (fecha consulta: 4.1.2015).

Consumer data privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf, (fecha consulta: 2.08.2014)

Big Data: seizing opportunities, preserving values, Executive Office of the President, The White House, 1.5.2014. http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf. (fecha consulta: 4.1.2015).

S.2588 Cybersecurity Information Sharing Act of 2014, 113th congress (2013-2014) 10.7.2014, https://www.congress.gov/bill/113th-congress/senate-bill/2588/text, (fecha consulta: 30.11.2014).

Consumer Privacy Bill of Rights Act of 2015, publicada el 27.2.2015, https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf (fecha consulta: 12.3.2015)

8. PRENSA

ABELLÁN, L., "EEUU presiona en la sombra para frenar la normativa de privacidad europea", *El País Internacional*, 21.7.2013, http://internacional.elpais.com/internacional/2013/07/21/actualidad/1374420934_701911.html, (fecha consulta: 20.7.2013).

CERF, V. "La lucha a favor de la libertad en internet", *El País, Opinión*, 3.12.2012 http://elpais.com/elpais/2012/11/29/opinion/1354207036_281116.html, (fecha consulta: 18.12.2012)

GARTON ASH, T. "La Red como campo de batalla", *El País, Opinión*, 11.12.2012 http:/elpais.com/elpais/2012/12/07/opinion/1354876187_848856.html (fecha consulta: 18.12.2012).

GIBBS, S., "*US court forces Microsoft to hand over personal data from Irish server*", *The guardian*, 29.4.2014, http://www.theguardian.com/technology/2014/apr/29/us-court-microsoft-personal-data-emails-irish-server (fecha consulta: 29.11.2014).

GREENWALD, G., "*XKeyscore: NSA tool collects' nearly everything a user does on the internet*", http://theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data/print y *Essential guide*, theguardian.com (fecha consulta: 31.7.2013).

HOWARD, D., *Corporate Vice President & Deputy General Counsel, Microsoft,* "*One step on the path to challenging search warrant jurisdiction", Microsoft on the Issues*, 25.4.2014, http://blogs.microsoft.com/on-the-issues/2014/04/25/one-step-on-the-path-to-challenging-search-warrant-jurisdiction/ (fecha consulta: 29.11.2014).

JIMÉNEZ CANO, R. "Google, acusado de manipular los resultados del buscador", *El País Economía*, 22.3.2015, http://economia.elpais.com/economia/2015/03/21/actualidad/1426913017_935765.html (fecha consulta: 8.4.2015).

MCNEAL, G. S. "*Controversial cybersecurity bill known as CISA advances out of Senate Committee*", *Forbes Business*, 9.7.2014,

http://www.forbes.com/sites/gregorymcneal/2014/07/09/controversial-cybersecurity-bill-known-as-cisa-advances-out-of-senate-committee/, (fecha consulta: 30.11.2014).

PÉREZ-LANZAC, C., RINCÓN, R., "Tu extimidad contra mi intimidad", *El País Archivo*, 24.3.2009, http://elpais.com/diario/2009/03/24/sociedad/1237849201_850215.html (fecha de consulta: 31.7.2013).

STREET, C. W., "*FTC leak suggests Google searches are biased, discriminatory", Breitbart California*, 21.3.2015, http://www.breitbart.com/california/2015/03/21/ftc-leak-suggests-google-searches-are-biased-discriminatory/ (fecha consulta: 8.4.2015).

VALENTINO-DEVRIES, J., SINGER-VINE, J., SOLTANI, A., *Websites vary prices, deals based on user's information, The Wall Street Journal*, 24.12.2012. http://online.wsj.com/articles/SB10001424127887323777204578189391813881534, (fecha consulta: 30.11.2014).

VÁZQUEZ, K. "Los bajos fondos de la red", *El País semanal Tecnología*, 14.8.2014, http://elpais.com/elpais/2014/08/13/eps/1407957234_037823.html (fecha consulta: 7.3.2015)

"Un ciberataque desde el televisor… e incluso desde un frigorífico" *El Mundo AFP*, 20.1.2014, http://www.elmundo.es/tecnologia/2014/01/20/52dce799ca4741d2548b4571.html, (fecha consulta: 1.12.2014).

"Un estudiante fuerza a Facebook a mejorar la privacidad", El País Tecnología, 25.12.2011, http://tecnologia.elpais.com/tecnologia/2011/12/25/actualidad/1324807261_850215.html (fecha consulta: 9.9.2015).

"Un estudiante lidera una demanda colectiva global contra Facebook" ABC Tecnología, Reuters, 3.8.2014, http://www.abc.es/tecnologia/redes/20140801/abci-estudiante-austriaco-demanda-global-201408011256.html, (fecha consulta: 9.9.2015).

9. OTRA NORMATIVA

State data protection Act Schleswig-Holstein 9 February 2000 GS Sch.-H. II, GI.Nr.204-4, https://www.datenschutzzentrum.de/material/recht/ldsg-eng.htm (fecha consulta: 12.8.2014)

Ley mexicana: Ley federal de protección de datos personales en posesión de los particulares, 5.07.2010, http://inicio.ifai.org.mx/LFPDPPP/LFPDPPP.pdf (fecha consulta: 5.8.2014).

Reglamento de desarrollo de la Ley mexicana: Reglamento de la ley federal (México) de protección de datos personales en posesión de los particulares, 21.12.2011, http://inicio.ifai.org.mx/PROTECCIONDEDATOSPERSONALES/RLFPDPP.pdf (fecha consulta: 5.8.2014).

10. OTROS DOCUMENTOS

Data protection accountability: the essential elements a document for discussion, October 2009, The Centre for Information Policy Leadership Hunton&Williams LLP.

Demonstrating and measuring accountability a discussion document, Accountability Phase II-The Paris project, October 2010, The Centre for Information Policy Leadership Hunton&Williams LLP.

Implementing accountability in the marketplace a discussion document, Accountability phase III-The Madrid project, November 2011, The Centre for Information Policy Leadership Hunton&Williams LLP.

Decision of the Bundesrat 52/12 30.3.2012 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012)11 FINAL; Council document 5853/12, http://www.bundesrat.de/SharedDocs/downloads/EN/uebersetzungen/0052-12b-en.pdf;jsessionid=EF0BF5125BC4D2C5B8BA3C1018DFB362.2_cid374?__blob=publicationFile&v=1, (fecha consulta: 5.12.2014).

Cámara de Diputados italiana. *Reasoned opinion, Proposal for a regulation of the European Parliament and of the Council on the protección of individuals with regard to the processing of personal data and on the free movement of such data (COM(2012)11 Final).*

EU data protection law: a "right to be forgotten"?, House of Lords, European Union Committee, 2nd Report of Session 2014-15, ordered to be printed 23 July 2014 and published 30 July 2014, pp. 8, 13-14, 21-22 y *European Union Committee, Home affairs, health and education sub-committee, EU data protection law: a "right to be forgotten"? Evidence*

PARISIER, E, Conferencia TED de *Beware online "filter bubbles"*, http://www.youtube.com/watch?v=B8ofWFx525s (fecha consulta: 27.10.2014)

PERRY BARLOW, J., Declaración de Independencia del Ciberespacio, http://es.wikisource.org/wiki/Declaraci%C3%B3n_de_independencia_del_ciberespacio, (fecha consulta: 28.11.2014).

Comment of The Sedona Conference Working Group 6 to Article 29 Data Protection Working Party Working Document 1/2009 (WP 158), October 30, 2009.

The Sedona Conference International Principles on Discovery, Disclosure&Data Protection: Best practices, recommendations&principles for addressing the preservation discovery of protected data in U.S. litigation, A project of the Sedona Conference Working Group 6 on International Electronic Information Management, Discovery&Disclosure (WG6), European Union Edition, public comment version, December 2011.

Propuesta conjunta para la redacción de estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal, adoptada en Madrid en 2009, http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_es.pdf, (fecha consulta: 2.08.2014).

ISO/IEC 29100:2011(E), *Joint Technical Committee* ISO/IEC JTC 1, *Information technology, Subcommittee SC 27, IT Security techniques*.

UNE-ISO/IEC 27001:2014 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información (SGSI). Requisitos.

Unlocking the value of personal data: from collection to usage, World Economic Forum, February 2013, http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf (fecha consulta: 7.3.2015).

Netmundial multistakeholder statement, 24 de abril de 2014, http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf (fecha consulta: 19.10.2014)

Security guidance for critical areas of focus in cloud computing v3.0, Cloud Security Alliance, 2011, https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf (fecha consulta: 22.8.2014)

Europe's Highest Court delays decisión in safe harbor case Schrems vs. Facebook, 10.6.2015, Hunton&Williams LLP, 2015, https://www.huntonprivacyblog.com/2015/06/10/europes-highest-court-delays-decision-safe-harbor-case-schrems-vs-facebook/ (fecha consulta: 9.9.2015).

ANEXOS

ANEXO I: **DEFINICIONES LEGALES DEL RESPONSABLE EN LA NORMATIVA MULTINIVEL**

1. UNIÓN EUROPEA

1.1. Textos vigentes

Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

> "responsable del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario;" (art. 2.d)

Reglamento 45/2001 para la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos

> "«responsable del tratamiento»: la institución, organismo, dirección general, unidad u otra entidad organizativa comunitaria que por sí sola o conjuntamente con otras determine los fines y los medios del tratamiento de datos personales; cuando los fines y los medios del tratamiento estén determinados por un acto comunitario concreto, el responsable del tratamiento o los criterios específicos aplicables a su nombramiento podrán determinarse en tal acto comunitario;" (art. 2.d)

Decisión marco 2008/977/JAI relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal

> "responsable del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; (art. 2.i)

1.2. Textos preparatorios

Propuesta de Directiva del Consejo relativa a la protección de las personas en lo referente al tratamiento de datos personales, COM(90) 314 final, DO C 277 de 5.11.1990, pág. 3.

> "responsable del fichero, la persona natural o jurídica, autoridad pública, servicio o cualquier otro organismo que, con arreglo al Derecho Comunitario o a la legislación de un Estado miembro, sea competente para decidir la finalidad del fichero, qué categorías de datos personales deben registrarse, qué operaciones deben aplicárseles a éstos y a qué terceros está permitido el acceso a los mismos;" (art. 2.e)

Propuesta modificada de Directiva del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, COM (92) 422 final, DO C 311 de 27.11.1992, pág. 30.

"responsable del tratamiento, la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate u ordene tratar datos personales y decida acerca de la finalidad y los objetivos del tratamiento, los datos personales que deben tratarse, las operaciones que deben aplicárseles y los terceros que pueden tener acceso a dichos datos;" (art. 2.d)

Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), 25.1.2012.

"«responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines, condiciones y medios del tratamiento de datos personales; en caso de que los fines, condiciones y medios del tratamiento estén determinados por la legislación de la Unión o de los Estados miembros, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por la legislación de la Unión o de los Estados miembros;" (art. 4.5).

Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos).

"«responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines y medios del tratamiento de datos personales; en caso de que los fines y medios del tratamiento estén determinados por la legislación de la Unión o de los Estados miembros, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por la legislación de la Unión o de los Estados miembros;" (art. 4.5).

Nota de la Presidencia al Consejo sobre Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)-Preparación de un planteamiento general, Expediente interinstitucional: 2012/2011 (COD) 9565/15, Bruselas, 11.6.2015.

"«responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines y medios del tratamiento de datos personales; en caso de que los fines y medios del tratamiento estén determinados por la legislación de la Unión o de los Estados miembros, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por la legislación de la Unión o de los Estados miembros;" (art. 4.5).

2. LEGISLACIÓN NACIONAL DE LOS PAÍSES OBLIGADOS A TRANSPONER LA DIRECTIVA 95/46/CE[1763]

2.1. Textos vigentes

Ley alemana: *Federal Data Protection Act 14 January 2003*

> "responsable del tratamiento: cualquier persona u órgano que recoge, trata o usa datos personales en su propio nombre o que lo encarga a otros" (Traducción de la autora art. 3.7 versión inglesa)

Ley austríaca: *Federal Act concerning the protection of personal data (DSG 2000)*

> "responsable del tratamiento: persona física o jurídica, grupo de personas u órgano de una entidad corporativa territorial (Gebietskörperschaft) o las oficinas de estos órganos, si deciden individual o conjuntamente con otros utilizar datos (sub-parágrafo 8) independientemente de que los datos los utilicen ellos mismos (sub-parágrafo 8) o que lo encomienden a un proveedor de servicios (sub-parágrafo 5). Seguirán considerándose responsables cuando aquellos proveedores de servicios a los que se haya encomendado llevar a cabo una tarea (sub-parágrafo 5) decidan utilizar los datos para esa finalidad (sub-parágrafo 8) excepto si esta utilización fue expresamente prohibida o si el contratado ha decidido bajo su propia responsabilidad en virtud de lo establecido en la ley o en códigos de conducta." (Traducción de la autora de parágrafo 4.4 versión inglesa).

Ley belga: *Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*

> "Por "responsable del tratamiento" se entiende la persona física o jurídica, la asociación de hecho o la administración pública que, sola o conjuntamente con otras, determina los fines y los medios del tratamiento de datos de carácter personal. Cuando los fines y los medios del tratamiento se determinen por o en virtud de una ley, de un decreto o de una ordenanza, el responsable del tratamiento será la persona física, la persona jurídica, la asociación de hecho o la administración pública designada como responsable del tratamiento por o en virtud de esta ley, de este decreto o de esta ordenanza." (Traducción de la autora art. 1.4).

Ley búlgara: *Law for protection of personal data January 2002*

> ""responsable de datos personales", en adelante referido como responsable de datos, será todo individuo o persona jurídica, o autoridad del gobierno central o local que determine de forma separada o conjuntamente con otra persona los fines y medios del tratamiento de datos personales.
> "un responsable" será también todo individuo o persona jurídica, o autoridad del gobierno central o local que determine de forma individual el tipo de datos personales tratados, los fines y medios del tratamiento de datos personales."
> "un responsable de datos" será también todo individuo o persona jurídica, o autoridad del gobierno central o local que trate datos personales cuyo tipo, fines y medios del tratamiento se determinen por ley. En estos casos, el responsable de datos o los criterios específicos para determinarlo podrán ser establecidos por una ley." (Traducción de la autora art. 3, apdos 1 y 2 versión inglesa).

[1763] Hay que tener en cuenta que las versiones no originales de las leyes provienen de traducciones realizadas en su mayoría por las autoridades de control y se trata de versiones no oficiales de las leyes que pueden ser textos no vigentes o que no coincidan fielmente con su original

Ley croata: *Personal data protection Act 17 September 2012*

> "responsable de fichero de datos personales: una persona física o jurídica, estado u otro órgano que determina los fines y los medios del tratamiento de datos personales. Cuando los fines y los medios del tratamiento se hubieran regulado por ley, la misma ley designará al responsable de fichero de datos personales" (Traducción de la autora art. 2.4 versión inglesa)

Ley checa: *Personal Data Protection Act, Act No. 101/2000 Coll. of April 4, 2000 on the protection of personal data and on amendments to some Acts*

> "responsable del tratamiento será cualquier entidad que determine los fines y medios del tratamiento de datos personales, lleva a cabo este tratamiento y es responsable del mismo. El responsable podrá apoderar o encargar a un encargado del tratamiento que trate datos personales, a no ser que una ley específica establezca lo contrario" (Traducción de la autora art. 4.j versión inglesa).

Ley chipriota: *The processing of personal data (protection of individuals) law 138(1) 2001*

> "responsable del tratamiento es cualquier persona que determina la finalidad y los medios del tratamiento de datos personales" (Traducción de la autora art. 2 versión inglesa).

Ley danesa: *Act on Processing of Personal Data (Act No. 429 of 31 May 2000*)

> "responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales" (Traducción de la autora art. 3.4 versión inglesa).

Ley de Liechtenstein: *Data Protection Act of 14 March 2002*

> "responsable del fichero o responsable: las personas privadas o autoridades que deciden sobre la finalidad y el contenido del fichero" (Traducción de la autora art. 3.1.k versión inglesa).

Ley eslovaca: *Act No. 122/2013 Coll. on personal data protection and on changing and amending of other acts, resulting from amendments and additions executed by the Act No. 84/2014 Coll*

> "responsable del tratamiento: cualquier entidad que sola o conjuntamente con otras determina los fines y los medios del tratamiento de datos personales, determina las condiciones del tratamiento y trata datos personales en su propio nombre; si la finalidad, o incluso las condiciones del tratamiento de datos personales se establecieran por una ley específica, por una norma directamente aplicable y legalmente vinculante de la Unión Europea o por un tratado internacional que obligue a la República de Eslovaquia, el responsable es aquel que para cumplir con la finalidad del tratamiento de datos personales sea designado como responsable o que cumpla con las condiciones establecidas por la ley, por la norma directamente aplicable y legalmente vinculante de la Unión Europea o por el tratado internacional que obligue a la República de Eslovaquia" (Traducción de la autora sección 4.2.b versión inglesa).

Ley eslovena: *Personal Data Protection Act (ZVOP-1*) *15 July 2004*

> "responsable de los datos es la persona física o jurídica u otra persona del sector público o privado que sola o juntamente con otras determina los fines y los medios del tratamiento de datos personales o una persona que designa una ley que también determina los fines y los medios del tratamiento" (Traducción de la autora art. 6.6 versión inglesa).

Ley estonia: *Personal Data Protection Act 15 February 2007*

> "Encargado del tratamiento de datos personales. (1) Un encargado del tratamiento de datos personales es una persona física o jurídica, la filial de una empresa extranjera o una agencia de gobierno local o estatal que trata datos personales o en cuyo nombre se tratan datos personales. (2) Un encargado del tratamiento determina: 1) los fines del tratamiento de datos personales, 2) las categorías de datos personales tratados, 3) el procedimiento y la forma del tratamiento de datos personales; 4) la autorización para comunicar datos personales a terceros. (3) Un encargado del tratamiento (de ahora en adelante encargado jefe) podrá autorizar por un acto administrativo o contrato, que otra persona o servicio (de ahora en adelante encargado del tratamiento autorizado) trate datos personales, a no ser que establezca lo contrario una ley o una regulación. (4) El encargado jefe proporcionará al encargado del tratamiento autorizado instrucciones obligatorias para el tratamiento de datos personales y será responsable del cumplimiento del encargado del tratamiento autorizado de los requisitos relativos al tratamiento de datos personales. En encargado jefe determinará los requisitos especificado en la subsección (2) de esta sección para el encargado del tratamiento autorizado. (5) El encargado del tratamiento autorizado podrá delegar la tarea del tratamiento de datos a otra persona sólo con el consentimiento por escrito del encargado jefe, siempre que esto no exceda los límites de la autoridad del encargado del tratamiento autorizado. (6) Un encargado del tratamiento que opere fuera de la Unión Europea que utilice medios ubicados en Estonia para el tratamiento de datos deberá designar un representante en Estonia, excepto en el caso especificado en la cláusula 2(1) 2) de esta ley." (Traducción de la autora art. 7 versión inglesa).

Ley finlandesa: *Personal Data Act 523/1999*

> "Responsable del tratamiento es una persona, empresa, institución o fundación, o varias de ellas, para quienes, con el fin de que lo utilicen, se establece un fichero y quienes están capacitadas para determinar el uso del fichero, o quienes hayan sido designadas como responsables por una ley" (Traducción de la autora art. 3.4 versión inglesa).

Ley francesa: *Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée*

> "El responsable de un tratamiento de datos de carácter personal es, salvo designación expresa por las disposiciones legislativas o reglamentarias relativas a este tratamiento, la persona, la autoridad pública, el servicio o el organismo que determina sus finalidades y sus medios" (Traducción de la autora art. 3.I).

Ley griega: *Law 2472/1997 on the protection of individuals with regard to the processing of personal data*

> "responsable del tratamiento cualquier persona que determine el alcance y medios del tratamiento de datos personales, sea una persona física o jurídica, autoridad pública o agencia o cualquier otra organización. Cuando los fines y medios del tratamiento los determinen las leyes o regulaciones nacionales o comunitarias, el responsable o los criterios concretos para su nombramiento se designarán en la ley nacional o comunitaria" (Traducción de la autora art. 2.g) versión inglesa).

Ley Países Bajos: *Act of 6 July 2000, Bulletin of Acts, Orders and Decrees 302, containing rules regarding the protection of personal data or Dutch Persona Data Protection Act*

> "parte responsable será la persona física, persona jurídica, órgano administrativo o cualquier otra entidad que, sola o conjuntamente con otras, determine los fines y los medios para el tratamiento de datos personales" (Traducción de la autora art. 1.d versión inglesa).

Ley húngara: *Act CXII of 2011 on the right of informational self-determination and on freedom of information*

> "responsable del tratamiento significa persona física o jurídica, u organización sin personalidad jurídica que sola o conjuntamente con otros determina los fines y medios del tratamiento de datos; realiza y ejecuta decisiones concernientes al tratamiento de datos (incluyendo los medios utilizados) o contrata un encargado del tratamiento para ejecutarlo" (Traducción de la autora Sección 3.9 versión inglesa).

Ley inglesa: *1998 Data Protection Act, 16.7.1998*

> "responsable del tratamiento" significa, sin perjuicio de lo establecido en la subsección (4), una persona que (sola o conjuntamente o en común con otras personas) determina los fines para los que y la forma en que cualquier dato personal, es o será tratado"
> "cuando los datos personales se tratan sólo para fines para los que por o en virtud de una disposición legal es preciso que se traten, la persona en quien recaiga la obligación de tratar los datos que se impone por o en virtud de la disposición legal será a los efectos de esta ley considerado responsable del tratamiento" (Traducción de la autora art. 1 subsecciones 1 y 4).

Ley irlandesa: *Data Protection Act 1988 Data Protection Act 1988, Number 25 of 1988, updated to 30 March 2012*

> "Responsable del tratamiento es la persona que, sólo o conjuntamente con otros controle el contenido y uso de los datos personales" (Traducción de la autora art. 1.1).

Ley islandesa: *Act on the protection of privacy as regards the processing of personal data No. 77/2000 of May 10, 2000 or Data Protection Act*

> "Responsable del tratamiento: la parte que determina los fines del tratamiento de datos personales, los medios que se utilizan, el método del tratamiento y otros usos de los datos" (Traducción de la autora art. 2.4 versión inglesa).

Ley italiana: *Codice in materia di protezione dei dati personali, Decreto legislativo 30 giugno 2003, n. 196*

> "responsable", la persona física, la persona jurídica, la administración pública y cualquier otra entidad, asociación u organismo a quien competa, aunque sea conjuntamente con otro responsable, la decisión en relación a la finalidad, la modalidad de tratamiento de datos personales y los instrumentos utilizados, incluido todo lo relativo a las medidas de seguridad" (Traducción de la autora art. 4.f versión inglesa).

Ley letona: *Personal Data Protection Law* 23.3.2000

> "Responsable del tratamiento: persona física o jurídica, institución del gobierno estatal o local que determina los fines y los medios del tratamiento de datos personales y que es responsable por el tratamiento de datos personales de acuerdo con esta ley" (Traducción de la autora art. 2.9 versión inglesa).

Ley lituana: *Law on legal protection of personal data No I-1374, 11.6.1996*

> "Responsable de los datos será una persona jurídica o física que sola o juntamente con otras determina los fines y medios del tratamiento de datos personales. Cuando los fines del tratamiento de datos personales se establecen en leyes y otras disposiciones legales, el responsable de los datos y/o el procedimiento para su designación podrán establecerse en estas leyes o disposiciones legales" (Traducción de la autora art. 2.7 versión inglesa).

Ley luxemburguesa: *Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel*

"Responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales. Cuando los fines y los medios del tratamiento estén determinados por o en virtud de disposiciones legales, el responsable del tratamiento será determinado por o en virtud de criterios específicos conforme a las disposiciones legales" (Traducción de la autora art. 2.n).

Ley maltesa: *Data Protection Act Chapter 440, 2001*

"Responsable de datos personales o responsable es una persona que sola o juntamente con otras determina los fines y los medios del tratamiento de datos personales" (Traducción de la autora art. 2 versión inglesa).

Ley noruega: *Act of 14 april 2000 No. 31 relating to the processing of personal data or Personal Data Act*

"Responsable del tratamiento: la persona que determina la finalidad del tratamiento de datos personales y que medios se utilizarán" (Traducción de la autora art. 2.4 versión inglesa).

Ley polaca: *Act of august 29, 1997 on the protection of personal data*.

"responsable del tratamiento significa el órgano, unidad organizativa, establecimiento o persona al que se refiere al artículo 3, que decide sobre los fines y medios del tratamiento de datos personales" (Traducción de la autora art. 7.4 versión inglesa).

"1. La ley polaca se aplicará a las autoridades estatales, autoridades territoriales auto-gobernables y a unidades organizativas estatales y municipales. 2. También se aplicará la ley a: 1) órganos no públicos que lleven a cabo tareas públicas, 2) personas físicas y jurídicas y unidades organizativas que no tengan personalidad jurídica, si realizan alguna parte del tratamiento como parte de su negocio o actividad profesional o para llevar a cabo algún objetivo establecido legalmente. Todas estas entidades deben además estar ubicadas en el territorio de la República de Polonia o en un tercer país, si se utilizan en el tratamiento de datos medios técnicos ubicados en el territorio polaco" (Traducción de la autora art. 3 versión inglesa).

Ley portuguesa: *Act 67/98 of 26 october on the protection of personal data*

"Responsable del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias, el responsable del tratamiento será designado en la ley que establezca la organización o el funcionamiento o en los estatutos que rijan el órgano jurídico o estatutario competente para tratar los datos" (Traducción de la autora art. 3.d versión inglesa).

Ley rumana: *Law No. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data, amended and completed*

"Responsable de datos: cualquier persona física o jurídica, incluyendo autoridades públicas, instituciones y sus órganos jurídicos, que establezca los medios y finalidad del tratamiento de datos personales; si la finalidad y los medios del tratamiento de datos personales se establecen en una disposición legal, el responsable de datos será la persona física o jurídica designada

como responsable por esta disposición legal concreta" (Traducción de la autora art. 3.g) versión inglesa).

Ley sueca: *Personal Data Act 1998:204*

"responsable de datos personales: una persona que sola o junto con otras decide el fin y los medios del tratamiento de datos personales" (Traducción de la autora sección 3 versión inglesa).

2.2. Textos no vigentes

Ley sueca número 289 de 11 de mayo de 1973: *Data Lag 1973:289*

"cualquier persona que mantiene un fichero con el fin de llevar a cabo sus actividades estando el fichero bajo su control" (Traducción de la autora de Sección 1 versión inglesa)

Ley Federal Alemana, de 27 de enero de 1977: *Bundesdatenschutzgesetz*, BDGS

"organismo almacenante: toda persona o entidad […] que almacene datos para ella misma o los haga almacenar por otros"

Ley francesa de 1978: *Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)*

"la persona que presenta la solicitud y aquella que tiene poder de decidir la creación del tratamiento o, si esta reside en el extranjero, su representante en Francia" (Traducción de la autora del artículo 19.1).

"Toda persona que ordene o lleve a cabo un tratamiento de informaciones nominativas se obliga en relación a las personas concernidas a tomar todas las precauciones útiles con el fin de preservar la seguridad de las informaciones y especialmente a impedir que sean modificadas, dañadas o comunicadas a terceros no autorizados" (Traducción de la autora del artículo 29.1).

Ley de Austria de 18 de octubre de 1978: *Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten, Datenschutzgesetz 1978, DSG 1978*

"gestor de datos: todo titular de derechos o todo órgano o corporación que, por sí mismo o mediante operadores informáticos, tratare datos por medios electrónicos"

Ley de Luxemburgo de 1979, *Loi du 31 mars 1979 réglementant l´utilisation des données nominatives dans les traitements informatiques*

"propietario del banco de datos: la persona por cuya cuenta se lleva el banco y que dispone de éste"

3. INSTRUMENTOS INTERNACIONALES

3.1. Consejo de Europa

3.1.1. Textos vigentes

Convenio 108: Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal

"autoridad «controladora del fichero» significa la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley

nacional para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán". (art. 2.d))

3.1.2. Textos preparatorios

Reforma C108: *Abridged report, Council of Europe Ad hoc Committe on data protection (CAHDATA), 3rd meeting, CAHDATA(2014)RAP03Abr, Strasbourg, 3.12.2014*

"Responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio, agencia o cualquier otro organismo que solo o conjuntamente con otros tiene el poder de decisión respecto al tratamiento de datos" (Traducción de la autora art. 2.d Reforma C108)

3.2. Organización de Cooperación y Desarrollo Económico (OCDE)

Guía OCDE 2013: *Recommendation of the Council concerning Guidelines governing the protection of privacy and transborder flows of personal data (2013), C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79*

"Responsable de los datos es la parte que decide sobre el contenido y uso de los datos personales, sin tener en cuenta si los datos se recogen, almacenan, tratan o se comunican por esta parte o por un agente en su nombre" (Traducción de la autora punto 1.a)

3.3. Cooperación Económica Asia-Pacífico (APEC)

APEC Privacy Framework: *Asia-Pacific Economic Cooperation Privacy Framework*

"responsable de información personal es la persona u organización que controla la recogida, el mantenimiento, el tratamiento o uso de información personal. Se incluye la persona u organización que encargue a otra persona u organización la recogida, mantenimiento, tratamiento, uso, transferencia o comunicación de información personal por cuenta suya, pero se excluye la persona u organización que lleve a cabo estas funciones por instrucciones de otra persona u organización. También se excluye al individuo que recoge, mantiene, trata o usa información personal en conexión con asuntos personales, familiares o domésticos del propio individuo" (Traducción de la autora de la definición contenida en apdo. 10).

3.4. Propuesta de Madrid

Propuesta conjunta para la redacción de estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal, adoptada en Madrid en 2009

""persona responsable": persona física o jurídica, de naturaleza pública o privada que, sola o en compañía de otros, decida sobre el tratamiento" (art. 2.d)

ANEXO II: GLOSARIO DE DEFINICIONES EN LA DIRECTIVA 95/46/CE

Directiva 95/46/CE: Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

a) «datos personales»: toda información sobre una persona física idientificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;
b) «tratamiento de datos personales» («tratamiento»): cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción;
c) «fichero de datos personales» («fichero»): todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;
d) «responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario;
e) «encargado del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento;
f) «tercero»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento;
g) «destinatario»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios;
h) «consentimiento del interesado»: toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan.” (art. 2)

ANEXO III: GLOSARIO DE DEFINICIONES EN LA NORMATIVA ESPAÑOLA

1. TEXTOS VIGENTES

1.1. Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD)

"a) Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables.
b) Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
c) Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
d) Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
e) Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.
f) Procedimiento de disociación: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.
g) Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.
h) Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
i) Cesión o comunicación de datos: Toda revelación de datos realizada a una persona distinta del interesado.
j) Fuentes accesibles al público: Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación." (art. 3)

1.2. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD)

"a) Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento.
b) Cancelación: Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.
c) Cesión o comunicación de datos: Tratamiento de datos que supone su revelación a una persona distinta del interesado.

d) Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
e) Dato disociado: aquél que no permite la identificación de un afectado o interesado.
f) Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.
g) Datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.
h) Destinatario o cesionario: la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos.
Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
i) Encargado del tratamiento: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.
Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
j) Exportador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.
k) Fichero: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
l) Ficheros de titularidad privada: los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.
m) Ficheros de titularidad pública: los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.
n) Fichero no automatizado: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.
ñ) Importador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.
o) Persona identificable: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.
p) Procedimiento de disociación: Todo tratamiento de datos personales que permita la obtención de datos disociados.
q) Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
r) Tercero: la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.
Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
s) Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.
t) Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación,
consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
(…)
l) Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.
(…)
p) Usuario: sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico" (art. 5)

2. TEXTOS NO VIGENTES

2.1. Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD)

"Responsable del fichero: persona física, jurídica de naturaleza pública o privada y órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento" (art. 3.d)