Jorge VILLARINO MARZO

LA PRIVACIDAD EN EL ENTORNO DEL CLOUD COMPUTING

Tesis doctoral

dirigida por

Dr. Pablo GARCÍA MEXÍA

Universitat Abat Oliba CEU

FACULTAT DE CIÈNCIES SOCIALS

Programa de doctorado en Humanidades y Ciencias Sociales

Departamento de Derecho y Ciencias Políticas

2017

Resumen

La evolución tecnológica ha tenido un enorme impacto en los derechos fundamentales, dando lugar al nacimiento de la cuarta generación de derechos. Uno de estos derechos ha sido, sin duda, el derecho a la protección de datos. La privacidad constituye una de las grandes preocupaciones de la sociedad. Por esta razón, cualquier desarrollo tecnológico plantea nuevos retos a la regulación de la protección de datos

La computación en nube es una nueva realidad tecnológica caracterizada por la ubicuidad, la elasticidad, el dinamismo, la virtualización, la escalabilidad y el pago bajo demanda.

En este trabajo se analiza si la regulación actual del derecho fundamental a la protección de datos es válida para hacer frente a los retos que plantea la computación en nube o si es necesario un nuevo régimen jurídico

Resum

L'evolució tecnològica ha tingut un enorme impacte en els drets fonamentals, donant lloc al naixement de la quarta generació de drets. Un d'aquests drets ha sigut, sens dubte, el dret a la protecció de dades. La privacitat constitueix una de les grans preocupacions de la societat. Per aquesta raó, qualsevol desenvolupament tecnològic planteja nous reptes a la regulació de la protecció de dades.

La computació en núvol és una nova realitat tecnològica caracteritzada per la ubiqüitat, l'elasticitat, el dinamisme, la virtualització, l'escalabilitat i el pagament sota demanda.

En aquest treball s'analitza si la regulació actual del dret fonamental a la protecció de dades és vàlida per fer front als reptes que planteja la computació en núvol o si és necessari un nou règim jurídic.

Abstract

The technological evolution has had a great impact on fundamental rights, giving rise to the fourth generation of human rights. One of these has been, with no doubts, the right to data protection. Privacy is one of the main concerns of society. For this reason, any new technological development poses new challenges to data protection regulation.

Cloud computing is a new technological reality characterized by ubiquity, elasticity, dynamism, virtualization, scalability and pay on demand.

In this dissertation we will analyze if the current data protection regulation is valid to face the new challenges pose by cloud computing or if a new legal regime is mandatory.

Palabras claves / *Keywords*

Derechos de cuarta generación - Privacidad – Protección de datos – computación en nube – régimen jurídico – subcontratación – transferencias internacionales – acceso – derechos de los interesados

Drets de quarta generació – Privacitat – Protecció de dades – computació en núvol – règim jurídic – subcontractació – transferències internacionals – accés – drets dels interessats

Fourth generation rights – Privacy – Data protection – cloud computing – legal regime – subcontracting – international transfers – access – rights of the data subject

INTRODUCCIÓN

La progresiva adaptación del Derecho a la nueva realidad social no es algo nuevo. De hecho está en su propia esencia. Recordemos cómo para la filosofía jurídica de Robert Alexy, "*el Derecho tiene una doble naturaleza. Comprende necesariamente tanto una dimensión real o fáctica como una dimensión ideal o crítica. El aspecto fáctico se refleja en los elementos definitorios de la legalidad conforme al ordenamiento y de la eficacia social, y el ideal en el de la corrección moral*"[1]. Es decir, cualquier norma, para que pueda ser adjetivada como jurídica ha de reunir las notas de legalidad conforme al ordenamiento, eficacia social y corrección material. Precisamente el objetivo central de esta memoria de tesis doctoral ha sido tratar de determinar si el régimen jurídico del derecho a la protección de datos tal y como hoy día se encuentra regulado, cumple con dichas exigencias en el entorno del *cloud computing;* si por el contrario, por la particular idiosincrasia de la misma, se hace necesaria una regulación *ad hoc*; o si basta con una modulación que puede ser aportada a través de los pronunciamientos jurisprudenciales o la labor de *soft law* y de supervisión por parte de las diversas autoridades de protección de datos. Estamos ante un eslabón más de la cadena de retos que plantea la revolución tecnológica a la norma jurídica, y es necesario dar una respuesta que otorgue confiabilidad a los operadores económicos en particular y a la sociedad en general.

Y es que la evolución del desarrollo tecnológico en los últimos años ha tenido tal impacto en nuestra vida que ha exigido de una respuesta por parte de todos los poderes públicos. Frente a las doctrinas ciberanarquistas o ciberlibertarias, que tuvieron quizá su expresión más gráfica en la Declaración de derechos del Ciberespacio impulsada por John P. Barlow, el Poder se ha visto progresivamente impulsado a recurrir a los mecanismos de ordenación de la sociedad para intentar hacer frente al referido fenómeno. El Derecho, en cuanto que uno de estos mecanismos, quizá el principal, no podía quedar al margen de este fenómeno tecnológico. Ello ha contribuido a que sean ya muchas las voces que reconocen al Derecho de Internet una autonomía en cuanto que rama del Derecho.

Se trata de un Derecho transversal que ha tenido una evolución diversa: en ocasiones se ha recurrido a una progresiva adaptación de las normas ya existentes, caso por ejemplo del

[1] ALEXY, R., Hauptelemente meiner Philosophie des Rechts. Traducción de OLIVER LALANA, A.D, *DOXA, Cuadernos de Filosofía del Derecho*, 2009, núm. 32, p. 67-84.

Derecho Civil en el campo específico de la propiedad intelectual; o del Derecho Penal, con la cada vez mayor presencia de la realidad tecnológica en los tipos delictivos. En otros casos, nos hemos encontrado con una regulación *ex novo* como ha ocurrido, por ejemplo, con todo lo concerniente al derecho a la protección de datos entendido en sentido amplio.

Como hemos apuntado, en el presente trabajo se busca analizar la repercusión en la protección de datos de una más de dichas evoluciones tecnológicas, el fenómeno de la computación en nube o del *cloud computing*. Se trata de un concepto metafórico que en sí mismo describe muy gráficamente ante lo que nos encontramos. Se ha considerado que es un campo idóneo para la investigación por tres motivos: en primer lugar porque ya han transcurrido casi quince años desde que apareciera por primera vez; porque se puede decir que desde hace casi una década se ha ido consolidando su presencia en la sociedad debido a su comercialización; y, en tercer lugar, porque todas las previsiones apuntan a que va a seguir creciendo, por lo que los retos que plantea en el ámbito jurídico van a seguir acompañándonos durante un tiempo.

Desde el punto de vista metodológico, a lo largo del trabajo se pretende mantener una homogeneidad en cuanto a las fuentes utilizadas, aunque lógicamente hay matices en los diferentes capítulos. Norma, jurisprudencia y doctrina han sido los pilares sobre los que se ha asentado esta investigación, recurriendo para ello lógicamente a las fuentes en español, pero inevitablemente y de una manera mayoritaria, a la jurisprudencia y la doctrina más allá de nuestras fronteras. Se han tenido en cuenta también las aportaciones llevadas a cabo por organismos oficiales, y en particular por las diversas autoridades de protección de datos que, a través de sus guías y documentos interpretativos, juegan un papel esencial a la hora de dotar de seguridad jurídica al régimen normativo del derecho a la protección de datos. Se ha trabajado en particular la doctrina norteamericana, en gran medida porque existe una larga tradición de estudio del ámbito normativo de internet, y porque el dominio del mercado por parte de los grandes proveedores de servicios de computación en nube corresponde a empresas norteamericanas. También en el plano doctrinal se han tenido en cuenta las aportaciones de distintos centros de investigación que tienen su foco en el Derecho de Internet y de grupos de trabajo específicos centrados en el ámbito del *cloud computing.* Por último, se ha de subrayar que se han manejado las aportaciones de los propios proveedores de servicios *cloud*, tanto divulgativas como empíricas, concretadas estas últimas en sus términos y condiciones de uso.

La memoria de tesis se estructura en esta introducción, cuatro capítulos, las conclusiones y un anexo en el que se recoge la bibliografía y las referencias jurisprudenciales nacionales, europeas y extranjeras. En los dos primeros capítulos se da el contexto de la investigación: una nueva generación de derechos fundamentales desde la perspectiva histórico-jurídica en el primero, y la nube como realidad tecnológica y económica en el segundo. Los otros dos capítulos van destinados a dar una respuesta jurídica a los principales retos que asume el derecho por excelencia de esa nueva generación, el derecho a la protección de datos, en el referido contexto tecnológico: la nube. En las conclusiones se reflejan de manera directa, tanto las respuestas parciales a cada uno de los retos descritos en los dos últimos capítulos, como la respuesta al objetivo central de la tesis: ¿es válido o no el régimen jurídico vigente para satisfacer las preocupaciones que para la privacidad puede plantear la nube? ¿Lo es sin modificación alguna o exige de una cierta flexibilidad?

Entrando a un mayor detalle, el objeto del primer capítulo ha sido analizar en qué medida las Tecnologías de la Información y de las Comunicaciones (TICs) han impactado en nuestro sistema de derechos fundamentales. Si llegáramos a la conclusión de que el impacto ha sido meramente evolutivo y no disruptivo, su interés como objeto de investigación se vería muy reducido. Además es necesario conocer dicho impacto para disponer de unos parámetros de comparación con la realidad a que luego ha dado lugar la computación en nube. Para lograrlo se ha partido de una de las clasificaciones, de las muchas que hay en el campo de los derechos fundamentales, más tradicionales: la de la generación de derechos. Tras una breve introducción, se analiza en qué medida el impacto de las TIC y de otros avances científicos –como la genética– ha dado lugar o no al surgimiento de una cuarta generación de derechos fundamentales y, en su caso, qué derechos, antiguos y modernos parafraseando a Constant, compondrían esa nueva generación de derechos. A efectos de la primera categoría se han analizado el derecho a la intimidad y el derecho a la libertad de expresión. El motivo de elegir estos dos derechos es que nadie niega su categoría de derechos fundamentales frente a otros muy afectados por Internet como puedan ser los derechos de propiedad intelectual o industrial, y porque se han visto particularmente afectados por Internet. A ello se añade que dicha afectación lo ha sido con un devenir opuesto, lo que como ahora se mencionará resulta de suma utilidad y muy enriquecedor a efectos de la investigación. El estudio se ha hecho desde una doble vertiente: temporal y geográfica. Desde el punto de vista temporal se ha trabajado en delimitar el núcleo esencial

de cada uno de esos dos derechos en su contenido tradicional, y desde el punto de vista geográfico se ha llevado a cabo el contraste entre dos visiones y tradiciones jurídicas que, a pesar de tener nexos en común, difieren en muchos aspectos: la europea y la americana. Desde el punto de vista metodológico, sin perjuicio de recoger la normativa existente, fundamentalmente textos constitucionales y convenciones internacionales de derechos, y de recurrir en determinadas ocasiones a la doctrina clásica, el eje de la investigación ha estado basado en la construcción jurisprudencial. El motivo principal es que han sido precisamente los tribunales los que han ido realizando una progresiva adaptación de la norma al contexto histórico, económico y sociológico existente en cada momento, recogiendo así la teoría hermenéutica de Savigny. En concreto se ha manejado principalmente la jurisprudencia del Tribunal Europeo de Derechos Humanos en el ámbito europeo y la del Tribunal Supremo en el caso de los Estados Unidos.

En la segunda parte del primer capítulo se ha profundizado en la evolución del factor tecnológico, con la finalidad de conocer en qué medida esta ha impactado en el contenido esencial de esos derechos, así como en sus técnicas de protección. En el ámbito concreto del derecho a la intimidad se han trabajado dos aspectos muy significativos en los que el efecto ha sido particularmente disruptivo: el entorno laboral y el de las investigaciones policiales y judiciales. En el caso de la libertad de expresión la atención se ha centrado fundamentalmente en el ámbito de la participación política, considerando que dicha libertad es básica en la construcción de una sociedad democrática. De nuevo ha tenido un papel central en la investigación la evolución jurisprudencial, aunque por razones cronológicas aquí hay un protagonismo añadido de otros tribunales como el Tribunal Constitucional, el Tribunal de Justicia de la Unión Europea o tribunales inferiores en el caso de Estados Unidos. Cuando ha resultado de interés para la investigación, se han incorporado también sentencias de otras latitudes de más de una decena de países, con la finalidad de verificar cómo la universalización del Derecho de Internet se puede estar llevando a cabo precisamente a través de los tribunales, frente a las dificultades que presenta la cooperación internacional normativa. En el marco de la libertad de expresión hemos prestado especial atención, además, a algunos aspectos esenciales como la importancia del principio de neutralidad en la red o, muy en particular, el papel que juega el régimen de responsabilidad de los prestadores de servicios de intermediación, atendiendo tanto al escueto desarrollo normativo que este vital aspecto tiene como, fundamentalmente, a la doctrina que, a través de la casuística, han ido sentando los tribunales. Al margen de estos derechos fundamentales que

podríamos considerar como tradicionales, el capítulo se ha cerrado con el estudio del derecho por excelencia que ha irrumpido, con independencia de sus antecedentes, particularmente en los últimos treinta años: el derecho a la protección de datos, que es el protagonista por excelencia en el entorno de la nube y el que mayores retos plantea, de ahí su estudio. Se ha tratado su delimitación conceptual, fundamentalmente en cuanto a su diferenciación y la relación que tiene con el derecho a la intimidad; y sus principios esenciales, con base en la normativa, la jurisprudencia y, lógicamente, las aportaciones doctrinales. No obstante, el régimen jurídico propiamente dicho no se ha desarrollado más allá del referido enunciado de sus principios, por cuanto constituye el núcleo central del objeto de la investigación a la hora de tratar su aplicabilidad al ámbito del *cloud computing*.

De los distintos aspectos o retos que plantea la computación en nube, no se ha profundizado, por razones de disciplina académica, en los tecnológicos y los económicos. Sin embargo, su indisociable vinculación a este nuevo paradigma computacional, obvio en el primero de los casos y una realidad de facto en el segundo, han hecho que sea necesario su tratamiento desde una perspectiva no especializada. A ello se ha dedicado el segundo de los capítulos. Se trata de fijar el contexto de la investigación. Si la nube no es una nueva realidad tecnológica, pierde sentido analizar la peculiaridad; y el hecho de que se haya tratado el esquema de computación en nube B2B, exigía el sucinto análisis de su dimensión económica. Al tratarse de una memoria de tesis jurídica, el enfoque, sin perder el rigor, se ha limitado a explicar los conceptos de un modo que sea suficiente para centrar el "terreno de juego". Es necesario conocer de qué estamos hablando, de dónde viene y cuáles son las características principales del *cloud computing* en el plano tecnológico y en qué medida estamos ante un mero movimiento de marketing o si estamos ciertamente ante un nuevo paradigma de computación que justifique una atención aislada. Se ha tratado la perspectiva económica en un doble análisis, macroeconómico y microeconómico, dando un mayor desarrollo a este último por el particular impacto que este tipo de tecnología tiene en el ámbito de las PYMES. El capítulo se ha cerrado con una referencia a los retos que plantea el *cloud* desde el punto de vista tecnológico, cultural y de seguridad, dejando apuntados los desafíos en el ámbito específico de la privacidad que son el núcleo central del trabajo y a los que se dedica la segunda parte de la tesis.

En el tercer y cuarto capítulo, se ha recurrido, como no puede ser de otro modo, a la norma jurídica, en aquellos casos en que esta existía. Desde el punto de vista geográfico se ha

tomado como punto de partida la norma europea, por cuanto nos encontramos ante un campo de actuación en el que la perspectiva nacional se quedaría pequeña. La universalidad de la Red hace que la perspectiva tuviera que ser mundial, pero la practicidad y la realidad de las cosas exigen que nos hayamos centrado fundamentalmente en el contexto europeo. A ello se añade el criterio temporal y sin duda la próxima puesta en práctica de un Reglamento General de Protección de Datos, de directa aplicabilidad en todos los Estados Miembros de la Unión Europea, que invita a centrar la atención en ella. No olvidemos a mayor abundamiento que se trata de una norma que ha servido como modelo, o al menos como instrumento argumental, en otros países con los que, en ocasiones, ni siquiera compartimos sistema jurídico. Obviamente las menciones a la normativa española, cuando la especificidad, el detalle o la ausencia de referencia en Europa lo exigían, también se ha tratado. En muchas ramas del Derecho la jurisprudencia ha jugado un papel clave, pero tal y como ya se ha apuntado, en esta investigación, en muchos aspectos, ha sido determinante. Desde el punto de vista doctrinal se han tenido en cuenta a los autores que ya podemos considerar como clásicos en el ámbito del Derecho de Internet, así como ambiciosos proyectos de investigación en el ámbito del *cloud*. En línea con los criterios metodológicos señalados, se han tenido en cuenta los dictámenes, guías y resoluciones adoptadas por las autoridades de protección de datos. Se ha recurrido principalmente a los documentos aprobados por el denominado Grupo de Trabajo del artículo 29 como también por las autoridades nacionales, principalmente de España (AGPD), Francia (CNIL) y Reino Unido (ICO).

La estructura de estos capítulos ha pretendido tener una homogeneidad, tanto en el plano formal de la extensión, como en el plano material en cuanto a la construcción interna, incorporando siempre la norma, los criterios de las autoridades de protección de datos, las aportaciones doctrinales y el posicionamiento de la industria. A partir de ahí se elaboran las críticas y se apunta el criterio de la investigación que en todo caso se desarrolla en las conclusiones. Por razones estructurales, y aunque bien pudiera haber constituido un todo, se ha optado por diferenciar dos capítulos: uno destinado a tratar los elementos más subjetivos, y otro a aquellos que tienen una mayor problemática en el plano objetivo. En todo caso, todos ellos plantean retos jurídicos. Ir viendo si la actual normativa de protección de datos permite dar respuestas parciales a dichos retos, nos hace a su vez posible a lo largo de los dos capítulos ir descubriendo y asentando nuestra respuesta definitiva al objeto de la investigación.

Así, en capítulo III se ha estudiado cuál es el papel que asume cada una de las partes, proveedor y cliente (teniendo en cuenta un enfoque *B2B*) desde el punto de vista de la normativa de protección de datos. Se trata de una cuestión fundamental en tanto en cuanto será también determinante de la normativa aplicable y en gran medida, consiguientemente, de la jurisdicción competente, máxime tras un RGPD que tiende a universalizar la normativa europea. También se ha incluido aquí el contenido que debe tener el contrato suscrito entre las partes, recurriendo al contraste con contratos de proveedores actualmente existentes en el mercado. Por último se trata el núcleo esencial del *habeas data*, vertiente que constituye uno de los núcleos esenciales del derecho a la protección de datos, concretado en el acrónimo tradicional de los derechos ARCO. El capítulo termina con el tratamiento de uno de los novedosos derechos que ha incorporado el RGPD y que aparentemente puede tener una particular trascendencia en el ámbito del *cloud*: el derecho a la portabilidad de los datos. En todas estas cuestiones se plantea si la norma se ve tensionada o no por encontrarnos en el entorno de la computación en nube. En caso de que dicha tensión exista, se observa si ésta puede superarse con criterios de flexibilidad y adaptabilidad; o, en su caso, si se fuerza de tal modo la interpretación que estaríamos ante situaciones comparables a un uso alternativo del Derecho y consiguientemente ante la necesidad de un nuevo régimen normativo.

En el cuarto y último capítulo se han desarrollado las cuestiones más problemáticas, o al menos los retos que de manera más generalizada se considera que tiene la privacidad en el entorno *cloud*, marcados por un elemento consustancial a esta tecnología: la ubicuidad. En concreto se ha tratado el régimen de las transferencias internacionales de datos, bajo sus diferentes paraguas normativos. También se ha recogido la problemática de la subcontratación, íntimamente conectada a la anterior. Tal es su conexión, que se han estudiado dentro de un mismo apartado. Especial atención ha requerido el régimen de las medidas de seguridad, que constituye un elemento transversal que afecta a la totalidad del ciclo de vida de los datos y al que se le ha dado un enfoque jurídico, sin entrar por tanto en consideraciones de tipo tecnológico, salvo cuando la norma jurídica así lo exigía. El capítulo concluye con un elemento estrechamente vinculado al carácter transfronterizo que la provisión de servicios en nube presenta en muchas ocasiones: el acceso a la información por parte de las autoridades públicas. En este aspecto se ha prestado especial atención a la situación en los Estados Unidos por dos motivos: el pleno dominio del mercado antes

apuntado, y los escándalos de vigilancia masiva que han aquejado a algunos proveedores americanos en los últimos años. Ello no obsta para que se hayan tenido en cuenta ejemplos de países europeos con la finalidad de demostrar las similitudes existentes, incluyendo lógicas referencias a la normativa española al respecto. Al igual que en el capítulo anterior, también aquí se irá dando una respuesta jurídica progresiva a cada uno de los retos a los que la nube se enfrenta. Se recurrirá para ello a la normativa existente, validando el régimen jurídico vigente, apuntando soluciones flexibles u ofreciendo soluciones radicalmente nuevas en función del discurrir investigador.

Por último, las conclusiones de esta Memoria de Tesis Doctoral, pretenden dar respuesta de manera sistematizada a la pregunta que subyace en la presente investigación, la de si hace falta o no un régimen jurídico específico de protección de datos en el ámbito del *cloud computing*. En caso de que no haga falta, qué ámbitos o qué problemas específicos pueden exigir una modulación del régimen actual; y sí hace falta un nuevo marco normativo, qué características debe tener.

"We are all now connected by the Internet, like neurons in a giant brain"

Stephen Hawking

CAPÍTULO I: DERECHOS Y LIBERTADES EN EL ENTORNO TECNOLÓGICO

1 Las generaciones de derechos.

Afirma Alessandro Pizzorusso que de "generaciones" de derechos se habla para clasificar, según cual sea el predominio de su contenido normativo y sobre la base de su evolución histórica, los catálogos de derechos cuya tutela se asegura en documentos denominados cartas, declaraciones, etcétera, o en constituciones de tipo moderno[2]. Y es que son muchas las clasificaciones de derechos humanos que se han hecho doctrinalmente, si bien es cierto que probablemente una de las de mayor predicamento ha sido la referida a las generaciones de derechos[3], a la que nos referimos más por un ánimo descriptivo, histórico y evolutivo que por su proyección jurídica. Tradicionalmente se ha hablado de tres generaciones de derechos, marcadas tanto por el momento de su nacimiento a efectos de su adjetivación, como de su trasfondo filosófico a efectos de su contenido.

La primera de estas generaciones hunde sus raíces en la filosofía política de John Locke, si bien es cierto que marcada por el previo pensamiento filosófico estoico, del iusnaturalismo tomista e incluso, en cuanto a su subjetivación, en las figuras españolas de Francisco de Vitoria y "el defensor de los indios" Bartolomé de Las Casas. Es la generación de los derechos de libertad, construidos sobre la filosofía política liberal frente a las monarquías absolutas. El hombre lucha por el reconocimiento de unos derechos inalienables, vinculados a su propia condición humana sobre la base de una construcción iusnaturalista. Son la vida,

---

[2] PIZZORUSSO, A., Las generaciones de derechos, traducido por BERZOSA LÓPEZ, D., *Anuario Iberoamericano de Justicia Constitucional*, 2001, nº 5, p. 291 y 292.

[3] A pesar de que existen fuertes y autorizadas críticas a esta clasificación, caso de LAPORTA SAN MIGUEL, F.J., El concepto de derechos humanos, *Doxa. Cuadernos de Filosofía del Derecho*, 1987, nº 4, p. 23. Disponible en Web: http://www.cervantesvirtual.com/servlet/SirveObras/12837218659036051876657/cuaderno4/Doxa4_01.pdf. En una línea intermedia se sitúa, GONZÁLEZ ÁLVAREZ, R., Aproximación a los derechos de cuarta generación, Disponible en Web: www.tendencias21.net/derecho/attachment/113651/
Este autor, aun siendo crítico con la construcción generacional de derechos fundamentales, afirma que "…*se ha mostrado con sólida convocatoria para el estudio clasificatorio de los derechos humanos, y es que, es sólo ese sentido el que debe asignársele, y no confundirla como determinante vital del surgimiento y desarrollo de los derechos*…".

la libertad o la propiedad e incluso la idea ilustrada a la que llamaban los colonos americanos de la búsqueda de la felicidad[4].

La segunda de las generaciones es la de los derechos sociales de carácter prestacional, marcada doctrinalmente por las consecuencias de la revolución obrera, influenciada por el pensamiento de Marx y Engels, con primeras manifestaciones en los movimientos revolucionarios de mitad del XIX y que tiene sus primeras manifestaciones normativa y constitucional, junto a la colectivista Declaración de los Derechos del Pueblo Trabajador y Explotado, en la Carta de Querétaro y en la Constitución de Weimar, aunque cabría remontarse a la Constitución Francesa de 1793 obra de Robespierre con el reconocimiento de los socorros públicos (art. 21). Este salto, probablemente el más cualificado que se ha dado hasta ahora en la historia de los derechos fundamentales, suponía "dinamizar la significación de los derechos fundamentales al añadir, a su función de garantía de las libertades existentes, la descripción anticipadora del horizonte emancipatorio a alcanzar"[5].

Numerosos textos internacionales han plasmado estas dos generaciones de derechos. Encontramos los derechos de primera generación en los primeros artículos de la Declaración Universal de los Derechos Humanos, y a partir del artículo 22 se recogen los derechos económicos, sociales y culturales propios de la segunda generación de derechos. También en el ámbito de las Naciones Unidas están ambas generaciones claramente reflejadas en los Pactos de la década de los sesenta, esto es, el Pacto Internacional de Derechos Civiles y Políticos por un lado, y el Pacto Internacional de Derechos Económicos, Sociales y Culturales por otro; a los que se unen en el plano europeo la Convención Europea para la Protección de los Derechos Humanos y de las Libertades Fundamentales y la Carta Social Europea.

La tercera de las generaciones de derechos tiene su origen en la conocida distinción que elaboró el jurista checo-francés Karel Vasak quien en 1979 afirmaba que, frente a los derechos de primera generación, asentados en el principio de libertad; y los derechos de segunda generación, asentados en el principio de igualdad, los derechos de tercera

[4] Aparece recogida esta idea a lo largo de los escritos de "El Federalista". AA.VV. *The Federalist. A Commentary on the Constitution of the United States; Being a Collection of Essays Written in Support of the Constitution Agreed Upon September 17, 1787, by the Federal Convention*, editado por LODGE H.C, Nueva York, Putman's, 1889, 586 p. Disponible en web: www.forgottenbooks.com, 2008.

[5] PÉREZ LUÑO, A.E., *Los derechos fundamentales*, 5ª edición, Tecnos, 1993, Temas Clave de la Constitución Española, 240 p.

generación se sostienen sobre el principio de solidaridad[6]. Se trata del derecho a la libre determinación de los pueblos, del derecho al desarrollo, a un medio ambiente sano o del derecho a la paz. Existen no obstante discrepancias doctrinales respecto a su posible consideración como verdaderos derechos fundamentales[7]. Son derechos que encuentran su plasmación normativa a partir de la década de los setenta en algunos textos como la Constitución portuguesa de 1976 o la Constitución española de 1978.

Todos estas generaciones de derechos han venido informadas por la posición del ciudadano frente al Poder, a diferencia de lo que vamos a poder observar en el caso de la cuarta generación de derechos, que surge fruto de la evolución tecnológica. El impacto cualitativo o no de esta en nuestro sistema de derechos fundamentales nos servirá para compararlo luego –en el caso concreto del derecho a la protección de datos– con el que ha ocasionado en concreto la computación en nube.

2 El contexto en el que nacen los derechos de cuarta generación: el surgimiento y posterior expansión de Internet.

Como afirma García Mexía, no es posible desconocer que el Derecho es un producto cultural, un producto de sociedades, y que las culturas y las sociedades evolucionan y se transforman[8]. Internet es probablemente uno de los inventos que mayor impacto ha tenido en el desarrollo humano, ni siquiera comparable a la imprenta de Gutenberg, y ello ya no solamente por su surgimiento sino principalmente por su carácter cambiante, lo cual, como veremos, tiene una especial trascendencia en su repercusión en el ámbito de los derechos fundamentales. Estamos ante una obra de carácter jurídico, pero toda construcción normativa viene dada por un contexto por lo que, como paso previo, debemos hacer un breve análisis sobre el origen y posterior desarrollo de Internet, atendiendo exclusivamente a los principales hitos y siendo consciente de que la evolución sigue dándose en el momento de escribir estas líneas. En todo caso, previamente a entrar en el aspecto descriptivo y por la imposibilidad de descender a un detalle excesivo, es conveniente desmitificar algunos aspectos, ya que la historia de Internet, como apunta Abbate[9], encierra un número de

[6] ALGAN, B., Rethinking "Third Generation" Human Rights, *Ankara Law Review*, Summer, 2004, vol 1, nº 1, p. 124. Karel Vasak introdujo el concepto de las tres generaciones de los derechos humanos en su conferencia para el Instituto Internacional de Derechos Humanos, en Estrasburgo, 1979.
[7] Estas discrepancias aparecen bien recogidas en RUIZ MIGUEL, C., La tercera generación de derechos fundamentales, *Revista de Estudios Políticos*, abril-junio, 1991, nº. 72, p. 301 y ss.
[8] GARCÍA MEXÍA, P.L., *Derecho Europeo de Internet*, Netbiblo, 2009, p. 20.
[9] ABBATE, J., *Inventing the Internet,* Cambridge, Massachusetts, MIT Press, 1999, 264 p.

sorpresas y confunde algunas presunciones habituales: Internet no es reciente, sino que representa décadas de desarrollo; no surge originariamente para ser un medio de comunicación personal sino para permitir a los científicos superar las dificultades de ejecutar programas en ordenadores remotos; y no es la historia de un conjunto de inventores heroicos, sino un cuento de colaboración y conflicto entre un variedad notable de actores.

Internet tiene sus orígenes a finales de los años sesenta cuando el Departamento de Defensa de los Estados Unidos se planteó la posible vulnerabilidad de su sistema de comunicaciones. Hasta entonces, el Departamento de Defensa utilizaba el *switched telephone network* (STN)[10] como sistema de comunicación, definido por el *Federal Standard 1037C* como *domestic telecommunications network usually accessed by telephones, key telephone systems, private branch exchange trunks, and data arrangements*[11]. Se trataba por tanto de una tecnología denominada de conmutación de circuitos, (un circuito es una conexión entre llamante y llamado), que establecía enlaces únicos y en número limitado entre importantes nodos o centrales, con el consiguiente riesgo de quedar aislado parte del país en caso de un ataque militar sobre esas arterias de comunicación[12]. Esta situación llevó al Departamento de Defensa a encargar a su Agencia de Proyectos de Investigación Avanzados (ARPA en sus siglas en ingles[13]) el desarrollo de la tecnología de conmutación de paquetes[14] sobre la base de las ideas del americano Licklider[15] y del profesor Kleinrock[16].

ARPA desarrolló esta nueva tecnología denominada conmutación de paquetes, cuya principal característica reside en fragmentar la información, dividirla en porciones de una determinada longitud a las que se llama paquetes. Cada paquete lleva asociada una cabecera con datos referentes al destino, origen, códigos de comprobación, etc. Así, el

[10] Red telefónica conmutada (traducción libre).
[11] Red nacional de telecomunicaciones por lo general accesible por los teléfonos, centrales telefónicas, centralitas privadas y los arreglos de datos (traducción libre).
[12] Está información está recogida de la descripción que hace la *Internet Society* (ISOC) sobre los orígenes de Internet. No es unánime sin embargo la aceptación de que ARPANET se crease como una necesidad ante una posible guerra nuclear. Ver al respecto MARTÍNEZ DE VELASCO FARINOS, A., Los orígenes de Internet; en AA.VV. *Las Ciencias Sociales en Internet*, Mérida, Junta de Extremadura, 2001, p. 22.
[13] ARPA cambió su nombre en 1971 por DARPA (añadiendo la palabra *Defense* al principio). Posteriormente, en 1993, volvió a llamarse ARPA y en 1996 DARPA.
[14] El término "conmutación de paquetes" aparece por primera vez en 1966 por la obra de Donald Davies, quien trabajaba para el Laboratorio Físico Nacional del Reino Unido (NPL).
[15] J.C.R. Licklider, junto con Wesley Clark (ambos profesores del prestigioso Instituto Tecnológico de Massachusetts, MIT) habían aportado el concepto teórico de la Red Galáctica que proponía una red interconectada globalmente a través de la cual cada uno podría acceder desde cualquier lugar a datos y programas.
[16] Kleinrock se doctoró en el MIT con una tesis doctoral sobre conmutación de paquetes en 1961 y posteriormente sería contratado en la UCLA.

paquete contiene información suficiente como para que se le vaya encaminando hacia su destino en los distintos nodos que atraviese. El camino a seguir, sin embargo, no está preestablecido, de forma que, si una parte de la red cae o es destruida, el flujo de paquetes será automáticamente encaminado por nodos alternativos. Los códigos de comprobación permiten conocer la pérdida o corrupción de paquetes, procediéndose en el sentido a la recomposición de los paquetes[17].

A través de la aplicación de esta tecnología surge ARPANET, impulsada por L.G. Roberts[18]. Se trataba de una red que lograba la interconexión de cuatro macro ordenadores de diversas Universidades[19], gracias entre otras cosas a la tecnología desarrollada por la empresa BBN que fue la creadora de unos pequeños ordenadores, llamados IMP (*Interface Message Processor* u ordenadores de comunicaciones) que permitía el envío de mensajes entre los macro ordenadores y el control de las comunicaciones.

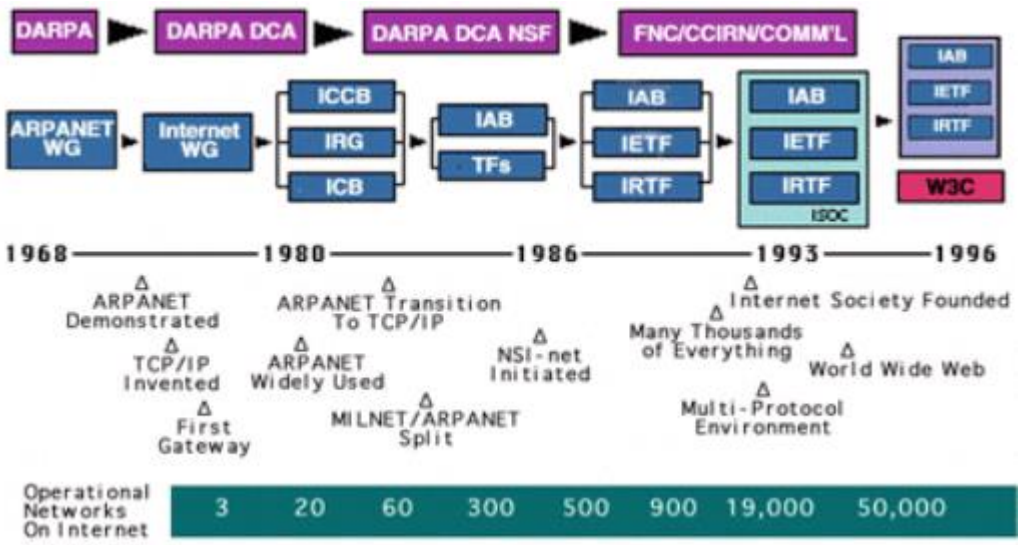
Probablemente el siguiente gran paso en la Historia de Internet vino marcado a mediados de los setenta por la creación por parte de Robert Kahn y Vinton G. Cerf de la serie de protocolos TCP (*Transmission Control Protocol*) e IP (*Internet Protocol*), correspondiendo al primero trocear en paquetes los mensajes generados en origen, recomponiéndolos en el nodo de destino; y al segundo la dirección de esos paquetes.

En 1983 se desgajó ARPANET de la parte relacionada con la defensa, que recibió el nombre de MILNET. De este modo, en 1983, con la utilización de los Protocolos TCP/IP nació Internet como red de interconexión entre ARPANET y otras redes como CSNET[20], a las que se añadirían otras en Estados Unidos y otros países. Es decir, se produce el gran cambio pasando de una red de ordenadores a una red de redes, que es la esencia de Internet.

En 1990, tras la caída del muro, desaparece el proyecto ARPANET y se consolida el concepto de Internet, como heredero único del proyecto original y herramienta determinante

[17] Paul Baran establecía el símil de la novela y las tarjetas postales: no se trataba de enviar una novela encuadernada, sino de enviar una novela escrita en tarjetas postales que el receptor de la misma se encargaría de reunir.
[18] L.G. Roberts trabajaba como investigador en el equipo de Kleinirock en la UCLA.
[19] Se trata de las Universidades de California en Los Ángeles, de California en Santa Bárbara, de Utah y el Instituto de Investigación de Stanford. DE ANDRÉS BLASCO, J., ¿Qué es Internet?; en GARCÍA MEXÍA, P.L, (Dir.), *Principios de Derecho de Internet*, 1ª edición, Tirant lo Blanch, 2005, p. 32.
[20] CSNET responde a las siglas de *Computer Science Network* y fue una red creada a principios de los ochenta para unir Departamentos de Ciencias Informáticas e instituciones académicas. Tuvo un papel importante en el desarrollo de Internet tal y como lo conocemos hoy, bajo la dirección de los profesores Denning (Universidad de Purdue), Farber (Universidad de Delaware) Hearn (Corporación RAND) y Landweber (Universidad de Wisconsin). http://en.wikipedia.org/wiki/CSNET

de la propia configuración del mundo hoy día. Las causas del crecimiento exponencial, señala De Andrés Blasco, fueron[21]: la política de puertas abiertas que permitió la libre conexión de todo tipo de organizaciones y de los propios usuarios particulares, la facilidad de interconexión que producía el protocolo TCP/IP, la absorción de otras redes de carácter más específico, como la citada CSNET o BITNET[22], y la incursión de los usuarios particulares, fundamentalmente a raíz de la aparición de los Proveedores de Servicios de Internet (PSI).



Fuente: ISOC[23]

[21] DE ANDRÉS BLASCO, ¿Qué es Internet?, ob. cit., p. 48.
[22] BITNET era una antigua red internacional de computadoras de centros docentes y de investigación que ofrecía servicios interactivos de correo electrónico y de transferencia de ficheros utilizando un protocolo de almacenaje y envío basado en los protocolos *Network Job Entry* de IBM. Se conectaba a Internet a través de una pasarela de correo electrónico.
Obtenido de "http://es.wikipedia.org/wiki/Bitnet"
[23] Para una sucinta explicación tecnológica de la historia de Internet, ver DELGADO KLOOS, C. y GARCÍA RUBIO, C., Historia de Internet; en CREMADES, J., FERNÁNDEZ ORDÓÑEZ, M.A, e ILLESCAS, R (Coords), *Régimen Jurídico de Internet*, La Ley-Actualidad, 2001, p. 87-100. Más detallado en DE ANDRÉS BLASCO, J., "¿Qué es Internet?", ob. cit. p. 29-97.

3 Repercusión jurídica de Internet y delimitación de nuestro estudio.

Son dos fundamentalmente los planos en los que los derechos y libertades se ven afectados por el surgimiento de las nuevas tecnologías y por los avances científicos en general: por un lado, el nacimiento de nuevos derechos (fundamentales) y por otro, su impacto en algunos de los ya existentes. Ambos forman –y aquí adelantamos ya nuestra conclusión– los derechos de cuarta generación[24]. La característica fundamental de esta nueva generación de derechos frente a las anteriores, como recoge muy acertadamente Gómez Sánchez, radica en que si las tres primeras generaciones son producto de la evolución política (aunque quizá la cuarta sea fruto del surgimiento como sugiere Frosini del poder informático[25]), la cuarta generación de derechos es producto de la evolución científica y técnica[26]. Una evolución que, como afirmara el profesor emérito del Instituto de Estudios Avanzados de Princeton, Freeman J. Dyson, está basada en tres pilares: el sol, el genoma e Internet[27], que conjuntamente tienen el potencial de crear una distribución más equitativa del bienestar mundial.

Efectivamente existe un debate abierto respecto a la existencia de los derechos de cuarta generación y a qué derechos formarían parte de esta nueva generación de derechos. Están por un lado quienes sostienen, como Bustamante Donás, que los derechos de cuarta generación son las nuevas formas que cobran los derechos de primera, segunda y tercera generación en el entorno del ciberespacio[28]. Frente a dicha postura está la de quienes

[24] No faltan voces como la del profesor Pérez-Luño que sitúa estos derechos como de tercera generación, englobando en la misma generación de derechos tantos los relacionados con las nuevas tecnologías como la conservación del medio ambiente natural, PEREZ LUÑO, A.E., Las generaciones de derechos humanos, *Revista del Centro de Estudios Constitucionales*, Septiembre-Diciembre 1991, nº 10, p. 203-217. En la misma línea ASPAS ASPAS, J.M., Derechos humanos y nuevas tecnologías: el derecho a la autodeterminación informativa; en CONTRERAS. M., POMED. L, y SALANOVA. R. (coord.), *Nuevos escenarios y nuevos colectivos de los derechos humanos. Conmemoración del cincuenta aniversario de la Declaración Universal de Derechos Humanos*, Monografías de la Revista Aragonesa de Administración Pública, 1998, p. 357-399. Igualmente SANZ LARRUGA, F.J., El Derecho ante las nuevas tecnologías de la información, *Anuario da Facultade de Dereito da Universidade da Coruña*, 1997, nº 1, p. 506 y ss; y también COTINO HUESO, L., Algunas claves para el análisis constitucional futuro de las libertades públicas ante las nuevas tecnologías (con especial atención al fenómeno de los «blogs»), en AA.VV. *Estudios jurídicos sobre la sociedad de la información y nuevas tecnologías*, Facultad de Derecho de Burgos, Burgos, 2005, p. 53.

[25] FROSINI. V., *Informática y Derecho*, traducción del italiano de GUERRERO, J. y AYERRA REDIN, M., Bogotá, Themis, 1988, 179 p.

[26] GÓMEZ SÁNCHEZ, Y., La protección de los datos genéticos: el derecho a la autodeterminación informativa, *Derecho y Salud*, vol. 16, nº extra 1, 2008 (Ejemplar dedicado a: XVI Congreso "Derecho y Salud"), p. 69.

[27] DYSON, F.J., *The Sun, the Genome and the Internet. Tools of Scientific Revolutions*, The New York Public Library, Oxford University Press, 1999, 144 p.

[28] BUSTAMANTE DONÁS, J., Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica, *Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Información*, septiembre 2001, nº 1, p. 3. Hay quienes consideran, como González Álvarez que “estas

sostenemos, como hemos apuntado, que los derechos de cuarta generación incluyen tanto un nuevo conjunto de derechos vinculados a la biomedicina y la genética por un lado (identidad genética, integridad genética, consentimiento informado en todas las intervenciones relacionadas con la salud…) y a las tecnologías de la información y de la comunicación por otro (el acceso universal a las nuevas tecnologías, la protección de datos personales….etc.). Como afirma Gómez Sánchez, los derechos de cuarta generación se caracterizan por su relación con nuevas tecnologías en general o biotecnologías en particular, hablando igualmente de la emergencia de nuevos derechos que vienen a dar respuesta a situaciones derivadas de la aparición y progresiva implantación de novedosas biotecnologías[29]. Pero también se integraría esta generación por aquellas facetas de los derechos de las anteriores generaciones que se han visto afectados de tal modo por la tecnología que han llegado a modificar los contornos de esos derechos y libertades y por tanto su contenido esencial. Una buena prueba de esta situación es que hay autores como Diaz Revorio que hablan de "intimidad genética"[30] o de "intimidad informática"[31]; y fuera de nuestras fronteras, lo mismo viene a sostener Lessig cuando define la *nueva arquitectura de la privacidad* a través de dos diferentes ideas: aquella parte de la vida de cada uno que es vigilada (*monitored*), y aquella parte de la vida de cada uno que puede ser buscada (*searchable*)[32], ambas ideas, se han visto claramente afectadas con motivo del surgimiento

propuestas no dejan de reflejar nuevos entornos de la actuación de los mismos derechos, sobre todo de los derechos civiles de primera generación como el de libertad de pensamiento o de expresión, y los culturales de segunda generación como el de gozar de los beneficios de la ciencia y tecnología, que salen a luz frente a nuevas amenazas como las restricciones del uso de Internet, la privacidad del servicio en línea...". GONZÁLEZ ÁLVAREZ, R., ob. cit.

[29] Además de la obra arriba citada, con mayor detalle y de la misma autora, GÓMEZ SÁNCHEZ, Y., *Derecho Constitucional Europeo: derechos y libertades*, 1ª ed., Madrid: Sanz y Torres, 2005, 499 p.

[30] El Tribunal Constitucional de Perú por ejemplo distingue la dimensión tradicional de la intimidad de la nueva dimensión genética. Así en su Sentencia de 21 de julio de 2014, afirma que "la orden de tomar una muestra del ADN del recurrente constituye una intervención 1 esta vez del derecho a la intimidad, no tanto por el hecho de la intervención corporal que ello supone [que, como antes se ha señalado, incide sobre el derecho a la integridad física], sino en razón del tipo de información que se puede obtener con la toma del componente químico del núcleo celular, que no comprende solo la información genética reveladora de la identidad de la persona, sino también la relacionada con la información de naturaleza codificante a partir de la cual es posible conocer cualquier otro dato o característica genética del sujeto al cual se practica el procedimiento [enfermedades, características, etc». Disponible en web: http://www.tc.gob.pe/jurisprudencia/2016/05312-2011-AA.pdf

[31] DÍAZ REVORIO, J., *Los Derechos Humanos ante los nuevos avances Científicos y Tecnológicos. Genética e Internet ante la Constitución*, Derecho y tic's, Tirant lo Blanch, 2009, p. 37. En la misma línea, ORZA LINARES, R.M., ¿Es posible la creación de nuevos derechos fundamentales asociados a las nuevas tecnologías de la información y de la comunicación?, En: a*ctas del IV Congreso Online del Observatorio para la Cibersociedad,* celebrado online del 12 al 29 de noviembre de 2009. Disponible en web: http://www.cibersociedad.net/congres2009/es/coms/es-posible-la-creacion-de-nuevos-derechos-fundamentales-asociados-a-las-nuevas-tecnologias-de-la-informacion-y-de-la-comunicacion/991/

[32] LESSIG, L. *The Arquitecture of Privacy*,Taipei, TaiwanNet 98, 1998, 23 p. Disponible en web: http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf

de las nuevas tecnologías. En fin, lo ha venido en reconocer nuestro Tribunal Constitucional, así por ejemplo en la Sentencia 70/2002 de 3 de abril. Aunque no llega a entrar realmente en el fondo de la cuestión, sí que deja constancia de su sensibilidad por ella en su FJ 9º: "Ciertamente los avances tecnológicos que en los últimos tiempos se han producido en el ámbito de las telecomunicaciones, especialmente en conexión con el uso de la informática, hacen necesario un nuevo entendimiento del concepto de comunicación del objeto de protección del derecho fundamental, que extienda la protección a esos nuevos ámbitos, como se deriva necesariamente del tenor literal del art. 18.3 CE".

Respecto a la primera cuestión, el reconocimiento normativo de derechos nuevos vinculados a la aparición de las nuevas tecnologías es, en el ámbito europeo, bastante reciente. Buena prueba de ello es que en el seno de lo que tradicionalmente se conoce como la Europa Occidental, el primer texto constitucional que recoge un derecho de esta naturaleza es la Constitución portuguesa de 1976, cuyo artículo 35 hace referencia al derecho a la protección de datos[33]. El segundo de estos textos es la Constitución española de 1978, cuyo artículo 18.4 se refiere a la denominada libertad informática[34]. Se trata en buena medida, por tanto, de derechos no recogidos en los textos constitucionales en la mayor parte de los ordenamientos europeos[35].

En este sentido es importante señalar que el reconocimiento jurídico del derecho a la protección de datos en el plano internacional tiene su primera plasmación en el Convenio para la protección de las personas físicas en relación con el tratamiento automatizado de datos personales (Convenio 108). Otro momento relevante en el ámbito internacional ha sido

[33] "1. Todos los ciudadanos tienen derecho a acceder a los datos informatizados que les conciernan, pudiendo exigir su rectificación y actualización, así como el derecho a conocer la finalidad a que se destinan, en los términos que establezca la ley.
2. La ley define el concepto de datos personales, así como las condiciones aplicables a su tratamiento automatizado, conexión, transmisión y utilización, y garantiza su protección, especialmente a través de una entidad administrativa independiente.
3. La informática no puede ser utilizada para el tratamiento de datos relativos a convicciones filosóficas o políticas, afiliación a partidos o sindicatos, confesión religiosa, vida privada y origen étnico, salvo con el consentimiento expreso del titular, autorización prevista por la ley con garantías de no discriminación o para procesamiento de datos estadísticos no indentificables individualmente.
4. Se prohíbe el acceso a datos personales de terceros, salvo en casos excepcionales previstos por la ley.
5. Se prohíbe la atribución a los ciudadanos de un número nacional único.
6. Se garantiza a todos el libre acceso a las redes informáticas de uso público, determinando la ley el régimen aplicable a los flujos de datos transfronterizos y las formas adecuadas de protección de datos personales y de otros cuya salvaguardia se justifique por razones de interés nacional.
7. Los datos personales que consten en ficheros manuales gozan de protección idéntica a la prevista en los apartados anteriores, en los términos que establezca la ley."
[34] "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".
[35] DÍAZ REVORIO, F. ob. cit. p. 37

el reconocimiento en la Carta de Derechos Fundamentales de la Unión Europea, ya que supone un paso adelante de trascendental importancia, puesto que implica efectos jurídicos para todos los Estados miembros de la Unión Europea, en cuanto que el Tratado de Lisboa le ha otorgado plenos efectos[36]. Incluso algún autor como Murillo de la Cueva y Piñar Mañas sostienen que este reconocimiento marca precisamente el comienzo de una etapa en la que la protección de datos de carácter personal se configura como un verdadero derecho fundamental autónomo e independiente del derecho a la intimidad[37], cuestión esta en la que nos vamos a detener con posterioridad. A ello cabría añadir nuevos derechos que si bien no han tenido tanto predicamento como el derecho a la protección de datos, sin embargo son condicionantes de muchos otros, como el derecho de acceso a Internet (al que nos referiremos posteriormente cuando hablemos de la libertad de expresión), que ha sido declarado, si bien de manera indirecta, como un derecho humano por Naciones Unidas[38], o por ejemplo el derecho al olvido que, si bien se encuentra íntimamente conectado al derecho a la protección de datos, ha adquirido una cierta sustantividad propia, caso del denominado derecho al olvido[39].

---

[36] El artículo 8 de la Carta dice: "Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. Estos datos se tratarán de modo leal, para fines determinados 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 la conciernan y a su rectificación. El respeto de estas normas quedará sujeto al control de una autoridad independiente". A juicio de algún autor, el derecho a la protección de datos adquiere sustantividad propia precisamente como consecuencia del reconocimiento normativo en esta Carta de Derechos, puesto que ya no se relaciona como en ocasiones anteriores con el derecho a la intimidad.

[37] LUCAS MURILLO DE LA CUEVA, P. y PIÑAR MAÑAS, J.L., *El derecho a la autodeternimación informativa*, Madrid, Fundación coloquio jurídico europeo, 2009, p. 93. En la misma línea Canales Gil afirma que el derecho a la protección de datos adquiere sustantividad propia precisamente como consecuencia del reconocimiento normativo en esta Carta de Derechos, puesto que ya no se relaciona como en ocasiones anteriores con el derecho a la intimidad. CANALES GIL, A., El derecho fundamental a la protección de datos de carácter personal, *Revista Jurídica de Castilla y León,* abril 2007, nº 12, p. 21.

[38] En mayo de 2011, Frank La Rue, ponente especial de Naciones Unidas para la promoción y protección del derecho a la libertad de opinión y de expresión, lo reflejó de manera indirecta en su informe señalando entre sus conclusiones que "dado que Internet se ha convertido en una herramienta indispensable para la realización de una amplia gama de derechos humanos, combatir la desigualdad, y acelerar el desarrollo y el progreso humano, asegurar el acceso universal a Internet debería ser una prioridad para todos los Estados". LA RUE F., *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Nueva York, Nacionas Unidas, 16 de mayo de 2011, 22 p. Disponible en Web. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf. Posteriormente, en el verano de 2016, Naciones Unidas adoptó una resolución no vinculante en la que el Consejo de Derechos Humanos de Naciones Unidas condenaba a los Estados que intencionadamente interrumpían el acceso a Internet. Acceso al texto de la resolución disponible en web: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

[39] El punto de inflexión en el reconocimiento de este derecho trae causa de la Sentencia en el denominado caso Costeja. Tribunal de Justicia de la Unión Europea. Caso Google Spain, S.L., Google Inc. y Agencia Española de Protección de Datos (AEPD), Mario Costeja González. (C-131/12), Sentencia de 13 de mayo de 2014. Disponible en web: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

En línea con nuestro concepto de derechos de cuarta generación, el segundo gran grupo de derechos que vamos a apuntar es el que surge de los cambios que las nuevas tecnologías han provocado en algunos derechos tradicionales, conectado con la teoría anglosajona de la *liberties' pollution*, término con el que se alude a la erosión y degradación que aqueja a ciertos derechos ante determinados usos de las nuevas tecnologías[40] y que parece haber sostenido, siquiera de manera indirecta, el Tribunal Supremo de los Estados Unidos cuando, como nos recuerda Leatherman, afirmaba hace ya más de una década que "…las diferencias en las características de los nuevos medios de comunicación justifican las diferencias en los estándares de la Primera Enmienda que les resultan aplicables"[41]. Sin perjuicio de derechos como el de la participación política a través de los mecanismos como el del voto electrónico[42], la libertad de creación artística con mecanismos como el de las redes *peer to peer* o el genérico derecho a la información, esencia de la Red como sistema de comunicación, nos vamos a centrar en dos derechos fundamentales sobre los que Internet ha tenido un particular impacto: el derecho a la intimidad y la libertad de expresión. Máxime cuando, como añade Chris Reed, se puede decir que basta un examen superficial para ver que los dos derechos más afectados por Internet, el derecho a la intimidad y la libertad de expresión, están en potencial conflicto entre sí[43], conflicto que por otro lado tiene una larga tradición en su versión no digital. Y es que efectivamente, como apunta García Mexía, mientras Internet constituye una indudable amenaza para los derechos a la intimidad y a la protección de datos, en gran medida lo contrario ocurre en relación con la libertad de expresión[44]. Todo

[40] ASPAS ASPAS, J.M., ob. cit., p.358. También en FERNÁNDEZ SEGADO, F., La dinamización de los mecanismos de garantía de los derechos y de los intereses difusos en el Estado social. *Boletín Mexicano de Derecho Comparado, Biblioteca Jurídica Virtual*, 1995, nº 83, p. 563-597.

[41] LEATHERMAN, B., *Internet Censorship and the Freedom of Speech*, American University, Washington D.C., 19 de mayo de 1999, Disponible en web: http://www.szasz.com/undergraduate/leathermanpaper.htm

[42] PECES-BARBA MARTÍNEZ, G., Los derechos fundamentales de naturaleza política y las nuevas tecnologías, en AA.VV., *Parlamento y nuevas tecnologías, II Jornadas parlamentarias de la Asamblea de Madrid*, Asamblea de Madrid, octubre 2001, p. 151 a 159.

[43] REED, C., *Internet Law,* 2nd Ed, Cambridge University Press*,* Law in Context, 2004, p. 256.

[44] GARCÍA MEXÍA, P.L., *Derecho Europeo de Internet*, ob. cit., p. 109. Esta idea de contradicción y de conflicto fluye en la propia esencia del ciberespacio. En este sentido el profesor Lima Torrado señala que "Pese a que hasta el momento la utilización de la red Internet y consiguientemente del ciberespacio ha consistido en un atentado permanente contra el sistema de derechos humanos se puede afirmar que hay elementos en el mismo que permiten abonar la idea de que se está empezando a utilizar en un sentido completamente opuesto. Potencialmente el ciberespacio puede servir de instrumento poderoso de garantía de los derechos humanos". LIMA TORRADO, J., Ciberespacio y protección de los derechos: ¿hacia una cibercultura de los derechos humanos?, *Cuadernos electrónicos de Filosofía del Derecho* [en línea], 2002, nº 5, Disponible en web: http://www.uv.es/CEFD/5/lima.html, I.S.S.N.: 1138-9877. En un sentido similar, el profesor Pérez Luño afirma que "En un mundo interdependiente, en el seno de sociedades interconectadas, la garantía de los derechos cívicos se halla en directa conexión, para bien o para mal, con los procesos que definen su instalación tecnológica. PÉREZ LUÑO, A.E., Nuevas tecnologías, informática y Derecho, en ASIS, R.D., BONDÍA, B., y MAZA, E., (coords.), *Los desafíos de los derechos humanos hoy*, Dykinson, 2007, p. 480.

ello sin perjuicio de que por la estrecha vinculación entre intimidad y protección de datos, tal y como luego veremos, no faltan abiertos conflictos tampoco entre la libertad de expresión y el derecho a la protección de datos reflejados de manera clara en la STJUE de 16 de diciembre de 2008 en el caso *Tietosujavaltuutettu* [45] en la que el TJUE se pronunciaba sobre la excepción del régimen de protección de datos si la divulgación se ejerce con fines exclusivamente periodísticos.

Debemos por tanto adentrarnos en una doble cuestión referida al derecho a la intimidad y a la libertad de expresión: ¿Qué es la intimidad y la libertad de expresión? y ¿en qué medida se han visto ambos derechos afectados por Internet? El acercamiento a las facetas del contenido que se han visto afectadas por Internet en ambos derechos requiere previamente un repaso a cuáles son los orígenes de estos derechos y su posterior desarrollo. El esquema que seguiremos será comparativo, con una descripción de sus características en los Estados Unidos y en Europa, recogiendo el ejemplo de España en algunas ocasiones, haciendo hincapié en los criterios jurisprudenciales que han ido modificando el contenido esencial de los dos derechos, todo ellos sin perjuicio de que esta labor tiene un carácter meramente

[45] Tribunal de Justicia de la Unión Europea. Caso Tietosujavaltuutettu c. Satakunnan Markkinapörssi Oy y otros (C-73/07), Sentencia de 16 de diciembre de 2008. Disponible en web: http://curia.europa.eu/juris/document/document.jsf?text=&docid=76075&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3668. Desde hace años, la sociedad Markkinapörssi recoge de la administración fiscal finlandesa datos públicos para editar anualmente extractos de dichos datos en las ediciones regionales del periódico Veropörssi. La información contenida en dichas publicaciones incluye el nombre y apellido de alrededor de 1.200.000 personas físicas cuyos ingresos superen determinados umbrales, así como, con un margen de aproximación de 100 euros, el importe de las rentas derivadas de sus rendimientos del trabajo y del capital, así como indicaciones relativas a la imposición de su patrimonio. La información se clasifica por municipio y por tipo de renta y se hace constar por orden alfabético. Markkinapörssi y Satamedia, una sociedad asociada, a la que se transmitieron los datos de que se trata en forma de discos CD-ROM, firmaron un acuerdo con una operadora de telefonía móvil que, por cuenta de Satamedia, estableció un servicio de mensajes de texto (SMS) que permite a los usuarios de teléfonos móviles recibir en su teléfono, por el pago de unos 2 euros, los datos publicados en el Veropörssi. A instancia del interesado, se eliminan los datos personales de dicho servicio. A raíz de las denuncias de particulares que alegaban la violación de su intimidad, el mediador encargado de la protección de datos, solicitó que se prohibiera a Markkinapörssi y Satamedia continuar las actividades relativas al tratamiento de datos personales controvertido. Entonces, el Tribunal Supremo de lo contencioso-administrativo, que debe resolver dicho asunto en última instancia, solicitó al Tribunal de Justicia de las Comunidades Europeas que se pronunciara sobre la interpretación acertada de la Directiva comunitaria 95/46/CE relativa a la protección de datos, pretendiendo esencialmente saber en qué circunstancias pueden considerarse las actividades controvertidas un tratamiento de datos realizado exclusivamente con fines periodísticos y, por tanto, ser objeto de las excepciones o restricciones a la protección de datos. El TJUE dijo que actividades como las que llevan a cabo Markkinapörssi y Satamedia relativas a los datos procedentes de documentos públicos según la legislación nacional, pueden calificarse de actividades periodísticas si su finalidad es divulgar al público información, opiniones o ideas por cualquier medio de comunicación. y consideró que es competencia del Tribunal Supremo contencioso-administrativo apreciar si las referidas actividades se ejercen exclusivamente con la finalidad de divulgar al público información, opiniones o ideas.
Ver un detallado comentario a esta Sentencia en LUCAS MURILLO DE LA CUEVA, P., y PIÑAR MAÑAS, J.L., ob. cit., p. 109 y ss.

instrumental en cuanto que punto de partida para poder analizar posteriormente el impacto que ha supuesto Internet en su contenido.

3.1 Los contenidos tradicionales del derecho a la intimidad y de la libertad de expresión.

3.1.1 El derecho a la intimidad.

La gran dificultad parte de qué debemos entender por intimidad. La definición clásica de Warren y Brandeis[46] habla de intimidad como *the right to be left alone* (el derecho a que "te dejen en paz")[47]. Sin embargo, como bien apunta Reed, no es posible vivir en sociedad sin interactuar con los demás[48]. Sin que exista la posibilidad de delimitar este contenido a nivel universal, lo vamos a comparar entre dos estándares, el norteamericano y el europeo[49] cuya relación, muy gráficamente es descrita por el profesor Whitman, como "el choque trasatlántico" y que a juicio del citado profesor de la Universidad de Yale se fundamenta en dos conjuntos de valores: por un lado, el interés europeo en la dignidad de la persona, amenazada fundamentalmente por los medios de masas; y de otro, el interés americano en la libertad, amenazada fundamentalmente por el gobierno[50].

---

[46] Ver la obra clásica sobre el derecho a la intimidad. WARREN, S.D. y BRANDEIS, L.D., The Right to Privacy*, Harvard Law Review*. December 15, 1890, Vol IV, nº 5, p. 193-220. No obstante Thomas Cooley ya había hablado de este derecho en el año 1888. COOLEY, T.M., *A Treatise on the law of torts, or the wrongs which arise independently of contract*, Edited by J. Lewis, 3rd ed, Chicago: Callaghan & Company, 1906, 592 p.

[47] Bob Sullivan cuenta que 6500 usuarios de MSNBC participaron en una encuesta para definir lo que entendían por privacidad o intimidad (la palabra inglesa *privacy*) y que lo más cercano a un consenso que se obtuvo fue la definición "Privacy is to be left alone"- SULLIVAN, B., *Privacy lost: Does anybody care?*, Disponible en web: http://www.msnbc.msn.com/id/15221095/print/1/displaymode/1098/

[48] REED, C., ob. cit., p. 262

[49] SULLIVAN, B., *La difference' is stark in EU, U.S. privacy laws*, Disponible en web: http://www.msnbc.msn.com/id/15221111/ns/technology_and_science-privacy_lost/
Nicole Wong, abogada de la compañía Google marca las diferencias de estándares cuando afirma que "el marco en Europa es el de la intimidad como un derecho fundamental; en Estados Unidos se aplica como un derecho de protección del consumidor". Estas declaraciones fueron hechas a raíz de la condena que los tribunales italianos impusieron a tres ejecutivos de Google como consecuencia de un video colgado en la Red en el que se hacía mofa de un chico autista. Ver la noticia en *New York Times* de 26 de febrero de 2010.

[50] WHITMAN, J.Q., The Two Western Cultures of Privacy: Dignity versus Liberty, *Yale Law Review*, marzo 2004, p. 1151 a 1221.
Una prueba clara del diferente concepto de intimidad, y aunque más vinculado al derecho a la protección de datos, es el denominado Acuerdo de "Puerto seguro". A fin de salvar estos enfoques de privacidad diferentes y proporcionar un medio simplificado a las organizaciones de EE.UU. para dar cumplimiento a la Directiva comunitaria sobre protección de la intimidad, el Departamento de Comercio de EE.UU., en consulta con la Comisión Europea, elaboró un marco denominado "puerto seguro" que fue admitido por la Comisión Europea mediante su Decisión de 26 de julio de 2000.

En los Estados Unidos, el concepto de privacidad ha ido evolucionando sobre la base del particular funcionamiento de su sistema jurídico[51]. Con independencia de la ya citada obra de Warren y Brandeis, y siguiendo a Gormley, podemos señalar que ha habido cuatro vertientes de la intimidad que han adquirido la suficiente solidez en la historia de los Estados Unidos como para poder considerarlas como asentadas, a saber[52]:

- El derecho a la intimidad con respecto a la adquisición y difusión de información sobre la persona, especialmente a través de la publicación no autorizada, la fotografía u otros medios. Es la construcción clásica de Warren y Brandeis (*Tort privacy*)[53] que se reflejó, entre otras, en la conocida Sentencia de la Corte Suprema de Nueva York *Marion Manola vs. Stevens & Myers* en junio de 1890[54].

- El derecho a la intimidad, con respecto a las búsquedas y confiscaciones gubernamentales que invaden la esfera individual en lo considerado razonable por la sociedad. (Cuarta Enmienda a la Constitución) que, con el antecedente del entonces ya Juez del Tribunal Supremo Luis Brandeis

El Acuerdo de "Puerto Seguro" constaba de siete principios básicos, referidos a la notificación (información a los afectados), opción (posibilidad de oposición de los afectados), transferencia ulterior a terceras empresas, seguridad, integridad de los datos (principios de finalidad y proporcionalidad), derecho de acceso y aplicación (procedimientos para la satisfacción de los derechos de los afectados). Estos principios permiten garantizar a los operadores que se adhirieran a los mismos una "presunción de adecuación" al nivel de protección exigido por la Directiva, permitiéndose así la libre transferencia internacional de datos a dichos operadores. Para ello, aquéllos debían manifestar ante la Oficina Federal de Comercio (u otra entidad por ella designada) su adhesión a estos principios y su compromiso de llevarlos a la práctica, adoptando para ello las medidas adecuadas. Tal y como veremos en esta obra, dicho Acuerdo se ha visto sustituido en julio de 2016 por el denominado “Escudo de Privacidad”.
Hoy día cabe mencionar que existen rigurosos informes que ponen de manifiesto, como veremos en algunas de los apartados posteriores de esta obra, en que se pone de manifiesto cómo las reformas de los últimos años hacen que esta afirmación este en cuestión y que el acercamiento sea mayor, particularmente en determinados ámbitos. Ver SIDLEY, *Essentially Equivalent. A comparison of the legal orders for privacy and data protection in the European Union and United States*, January 2016, 173 p., Disponible en web: http://www.sidley.com/~/media/publications/essentially-equivalent---final.pdf

[51] Una amplia y descriptiva relación de la evolución del derecho a la intimidad de los Estados Unidos en GORMLEY, K., One hundred years of privacy*, Wisconsin Law Review,* University of Wisconsin, 1992, nº 1335, p. 1335-1441.

[52] *Idem*.

[53] El concepto *Tort* vendría a ser un acto o daño (que no suponga una ruptura contractual) que puede dar lugar a una acción civil.

[54] Estados Unidos. Corte Suprema de Nueva York. Caso Marion Manola vs. Stevens & Myers. Sentencia de 15 de junio de 1890

en su voto particular en la Sentencia *Olmstead vs. United States*[55], se recogería en la Sentencia *Katz vs. United States* en 1967[56].

- El derecho a la intimidad, cuando la libertad de expresión de un individuo amenaza con perturbar la libertad de pensamiento y reposo de otro ciudadano (Primera Enmienda a la Constitución), plasmado en la Sentencia *Breard vs. City of Alexandria* de 1951[57].

- El derecho a la intimidad, con respecto a las decisiones fundamentales (a menudo no previstas) relativas al propio individuo, que son explícita o implícitamente reservadas a los ciudadanos (en vez de cedidas al gobierno) por los términos del contrato social, (Decimocuarta Enmienda a la Constitución) y que tendría su plasmación en la Sentencia *Griswold vs. Connecticut* del año 1965 que supuso un punto de inflexión en la configuración del derecho a la intimidad[58].

En todo caso, el sistema jurídico norteamericano sí tiene algún texto en el que se hace referencia expresa a la intimidad, como ocurre en el artículo 1, sección 1 de la Constitución

[55] A juicio de Lawrence Lessig "si hay una opinión para del Tribunal Supremo que debería ser modelo para los *ciberactivistas* en el futuro, si hay un primer capítulo en la lucha para proteger la intimidad en el ciberespacio, es esta sentencia, esta opinión y este caso. Aquí, en un ejemplo claro como ninguno, estamos ante un método que será clave para la supervivencia del ciberespacio como un lugar donde los valores de la libertad individual se mantengan. Brandeis trabajó primero para identificar los valores de la IV Enmienda original y, en segundo lugar, para trasladar esos valores en el contexto del ciberespacio", LESSIG, L., ob. cit., p. 7

[56] Estados Unidos. Tribunal Supremo. Sentencia Katz vs. United States. Sentencia de 18 de diciembre de 1967. Acceso al texto de la Sentencia en el siguiente enlace: https://supreme.justia.com/cases/federal/us/389/347/case.html

[57] Estados Unidos. Tribunal Supremo. Caso Breard vs. City of Alexandria. Sentencia de 4 de junio de 1951. Acceso al texto de la Sentencia en el siguiente enlace: https://supreme.justia.com/cases/federal/us/341/622/case.html

[58] Estados Unidos. Tribunal Supremo. Caso Griswold vs. Connecticut. Sentencia de 7 de junio de 1965. Acceso al texto de la Sentencia en el siguiente enlace: https://supreme.justia.com/cases/federal/us/381/479/case.html
En esta Sentencia se declaró inconstitucional la Ley del Estado de Connecticut que prohibía el uso de anticonceptivos a las personas casadas, considerándolo una conducta delictiva. La inconstitucionalidad se fundó en la violación del derecho a la intimidad.

del Estado de California; en el artículo 1, sección 10 de la Constitución de Montana o en la *Privacy Act* de 1974[59].

A diferencia de lo ocurrido en Estados Unidos, en España, y en el resto de las Constituciones europeas, el reconocimiento del derecho a la intimidad está plasmado en textos normativos, aunque bien es cierto que no en todos los casos hay una expresa mención constitucional[60]. En concreto el artículo 18.1 CE dice: "Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen". *Per se*, el citado artículo ya tiene un contenido. Sin embargo, al igual que acabamos de ver, la construcción del derecho a la intimidad ha estado influenciada por el desarrollo de una jurisprudencia constitucional que ha ido marcando en diferentes momentos, el contenido esencial de este derecho.

En un primer acercamiento, la STC 231/1988[61], dictada en el famoso caso *Paquirri*, afirmaba que "Los derechos a la imagen y a la intimidad personal y familiar reconocidos en el artículo 18 de la CE aparecen como derechos fundamentales estrictamente vinculados a la propia personalidad, derivados sin duda de la dignidad de la persona". Ahora bien, estos pronunciamientos que vinculan el derecho a la intimidad a la dignidad humana, no excluyen la posibilidad de que existan límites que también han sido marcados por la misma jurisprudencia constitucional, cuando el recorte que aquél haya de experimentar esté fundado en una previsión legal que tenga justificación constitucional y que sea proporcionada (SSTC 44/1999[62] o 207/1996[63]), o cuando exista un consentimiento eficaz que lo autorice, puesto que corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno (STC 83/2002[64]).

---

[59] Bien es cierto que este texto, como veremos, hace más bien referencia al tratamiento de datos personales por parte de las agencias federales en Estados Unidos y se alejaría más del concepto de intimidad que ahora estamos manejando.

[60] En Alemania se ha reconocido en el seno del derecho a la propia personalidad *(allgemeines Persönlichkeitsrecht*); en Italia ha sido una creación jurisprudencial hasta la ley 675/96 que fue fruto de las directivas comunitarias; mientras que en Francia se introdujo en el Código Civil en 1970. Ver CELIS QUINTAL, M.A., La protección de la intimidad como derecho fundamental de los mexicanos. En CIENFUEGOS SALGADO, D., y MACÍAS VÁZQUEZ, M.C. (Coords.), *Estudios en homenaje a Marcia Muñoz de Alba Medrano. Protección de la persona y derechos fundamentales*, Universidad Nacional Autónoma de México, 2006, p. 71-108, Disponible en web: http://www.bibliojuridica.org/libros/5/2253/9.pdf

[61] España. Tribunal Constitucional (Sala Segunda). Sentencia 231/1988 de 2 de diciembre. Acceso al texto de la Sentncia en el siguiente enlace: http://hj.tribunalconstitucional.es/eu/Resolucion/Show/1172

[62] España. Tribunal Constitucional (Sala Segunda). Sentencia 44/1999, de 22 de marzo. Acceso al texto de la Sentncia en el siguiente enlace: http://www.boe.es/diario_boe/txt.php?id=BOE-T-1999-9288

[63] España. Tribunal Constitucional (Sala Primera). Sentencia 207/1996, de 16 de diciembre. Acceso al texto de la Sentncia en el siguiente enlace: http://hj.tribunalconstitucional.es/ca/Resolucion/Show/3259

[64] España. Tribunal Constitucional (Sala Primera). Sentencia 83/2002, de 22 de abril. Acceso al texto de la Sentncia en el siguiente enlace: http://hj.tribunalconstitucional.es/el/Resolucion/Show/4619

Sin entrar, por exceder absolutamente del objeto de esta obra, en el estudio referido al debate que existe sobre el carácter formal o material del concepto de intimidad, esto es, sobre si a cada uno le corresponde marcar o fijar hasta dónde llega su privacidad o si bien es algo delimitado sobre la base de lo socialmente aceptado; sí que hay que reseñar que la jurisprudencia constitucional se ha ido pronunciando sobre ámbitos materiales concretos: el derecho a la intimidad abarca así la denominada intimidad corporal (STC 218/2002[65]); no abarca la faceta patrimonial (STC 76/1990[66] referida al secreto bancario); permite la videovigilancia de los trabajadores cuando sea absolutamente indispensable para proteger la seguridad de la empresa (STC 98/2000[67] referida a un casino de juego); o por ejemplo sí incluye las preferencias y conductas sexuales, llegando nuestro TC a considerar el acoso sexual en el centro de trabajo como una violación del derecho a la intimidad (STC 136/2001[68])[69].

3.1.2 La libertad de expresión.

El segundo de los derechos a los que vamos a atender es el derecho a la libertad de expresión. Dentro de las numerosas diferencias que hay entre los sistemas jurídicos europeo y norteamericano, probablemente aquí nos encontremos ante una de las más marcadas[70]. En los Estados Unidos la libertad de expresión se encuentra reconocida y garantizada en la I Enmienda, cuando dice: "El Congreso no hará ley alguna por la que adopte una religión como oficial del Estado o se prohíba practicarla libremente, o que coarte la libertad de palabra o de imprenta, o el derecho del pueblo para reunirse pacíficamente y para pedir al gobierno la reparación de agravios".

Se trata de una libertad esencial en la construcción de una sociedad democrática y se encuentra en el mismo corazón de la cultura norteamericana. Y es que, como dijera el Tribunal Supremo en 1974 "La Primera Enmienda no sólo sirve a las necesidades de la

[65] España. Tribunal Constitucional (Sala Primera). Sentencia 218/2002, de 25 de noviembre. Acceso al texto de la Sentncia en el siguiente enlace: http://hj.tribunalconstitucional.es/es/Resolucion/Show/4754
[66] España. Tribunal Constitucional (Pleno). Sentencia 76/1990, de 26 de abril. Acceso al texto de la Sentncia en el siguiente enlace: http://hj.tribunalconstitucional.es/ca/Resolucion/Show/1501
[67] España. Tribunal Constitucional (Sala Primera). Sentencia 98/2000, de 10 de abril. Acceso al texto de la Sentncia en el siguiente enlace: https://www.boe.es/boe/dias/2000/05/18/pdfs/T00041-00048.pdf
[68] España. Tribunal Constitucional (Sala Segunda). Sentencia 136/2001, de 18 de junio. Acceso al texto de la Sentncia en el siguiente enlace: http://hj.tribunalconstitucional.es/ca/Resolucion/Show/4432
[69] DÍEZ-PICAZO, L.M., *Sistema de derechos fundamentales*, Thomson-Civitas, 2003, p. 254 y ss.
[70] NÚÑEZ ENCABO, M., Europa y EE.UU: dos conceptos divergentes de la libertad de expresión, *Anuario de Derechos Humanos, Nueva Época*, 2008, Vol. 9, p. 461-478.

organización política, sino también a las del espíritu humano - un espíritu que exige la libre expresión"[71]. Con esta idea se conecta la metáfora del "mercado de las ideas", utilizada de manera continua por el Tribunal Supremo de los Estados Unidos en los casos sobre libertad de expresión y que trae causa de la construcción doctrinal del juez Oliver Wendell Holmes en su voto disidente en la Sentencia *Abrams vs. United States* (1919). Esta doctrina establecía que "el bien último de la sociedad se alcanza mejor a través del libre comercio de ideas y que la mejor prueba de la verdad es el poder del pensamiento para conseguir ser aceptado en la competencia del mercado"[72].

A pesar de este pronunciamiento de partida, la construcción de la libertad de expresión y más bien de los límites a la misma, se ha dado una vez más con el paso de los años a través de las decisiones jurisprudenciales, incluso en lo referido a su ámbito de aplicación. Así, en su Sentencia *Barron vs. Baltimore* en 1833[73], el Tribunal Supremo decretó que la Carta de Derechos sólo era vinculante para el gobierno federal. Sería en la Sentencia *Gitlow vs. New York* en 1925[74] cuando este mismo Tribunal modificó parcialmente dicha decisión al considerar que la mayoría de los derechos allí contemplados, incluida la libertad de expresión, eran también vinculantes para los gobiernos de los Estados, apoyándose en la cláusula del *due process of law* que recoge la XIV enmienda a la Constitución. Esta última Sentencia fue especialmente importante al marcar el ámbito de aplicación de la libertad de expresión y al pronunciarse sobre los posibles límites, en este caso basados en que en determinados supuestos el Estado puede castigar las expresiones que ponen en peligro los cimientos del gobierno y amenazan su derrocamiento por medios ilícitos.

Ahora bien, a pesar de la muy alta protección de la libertad de expresión en los Estados Unidos, también se han recogido determinados límites, entre otros[75]: la obscenidad, sobre la

[71] Ver el magnífico artículo de Rodney A. Smolla, Decano de la Facultad de Derecho de la Universidad de Richmond, sobre la importancia de la libertad de expresión en el sistema político norteamericano, SMOLLA R.A., *First Amendment Law Handbook*, Thomson-Reuters, 2014-2015, 628 p.
[72] La traducción es propia. Estados Unidos. Tribunal Supremo. Caso Abrams vs. United States. Sentencia de 10 de noviembre de 1919. Acceso al texto de la Sentencia en: http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=250&invol=616
[73] Estados Unidos. Tribunal Supremo. Caso Barron vs. Baltimore. Sentencia de 16 de febrero de 1833. Acceso al texto de la Sentencia en el siguiente enlace: https://supreme.justia.com/cases/federal/us/32/243/case.html
[74] Estados Unidos. Tribunal Supremo. Caso Gitlow vs. Nueva York. Sentencia de 8 de junio de 1925. Acceso al texto de la Sentencia en el siguiente enlace: https://supreme.justia.com/cases/federal/us/268/652/case.html
[75] *Freedom of Speech*, *Law Encycolpedia*.

base del conocido como test de Miller, establecido en el caso *Miller vs. California* en 1973[76]; las restricciones a las expresiones si se trata por ejemplo de palabras que van más allá de la protección de la Primera Enmienda, como es el caso de la incitación a la violencia inmediata; los discursos que presentan una acción ilegal inminente que fueron prohibidos inicialmente sobre la base del test de peligro claro e inmediato establecido por la Sentencia *Schenck vs. United States*[77], aunque esta prueba fue sustituida por la prueba de una acción fuera de la ley inminente establecida en el caso *Brandenburg vs. Ohio*[78], la difamación y la calumnia con base en la reducida definición de la difamación fijada en el caso de *Hustler Magazine vs. Falwell* (1988)[79] o las declaraciones hechas por los empleados públicos con arreglo a sus funciones oficiales tal y como marcó la Sentencia *Garcetti vs. Ceballos* (2006)[80], aplicable también para las empresas privadas que tienen al gobierno como cliente.

En Europa, la CEDH recoge en su artículo 10 la referencia a la libertad de expresión[81]: "1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas, sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. El presente artículo no impide que los Estados sometan a las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa".

---

[76] Este Test fue elaborado en la citada sentencia (cuyo resultado fue muy ajustado, en concreto 5 a 4) por el ponente de la mayoría, el Magistrado Warren Burger y estableció los criterios para considerar si una determinada obra era obscena y consiguientemente no estaba protegida por la I Enmienda. En concreto aludía a un triple criterio: si una persona media, atendiendo a los criterios sociales, consideraría que la obra, en su conjunto, apela al interés lascivo; si la obra representa o describe, de una manera patentemente ofensiva, una conducta sexual específicamente definida por la ley estatal aplicable y si la obra, en su conjunto, carece de valor literario, artístico, político o científico. Estados Unidos. Tribunal Supremo. Caso Miller vs. California. Sentencia de 21 de junio de 1973. Acceso al texto de la Sentencia en el siguiente enlace: https://supreme.justia.com/cases/federal/us/413/15/case.html

[77] Estados Unidos. Tribunal Supremo. Caso Schenk vs. United States. Sentencia de 3 de marzo de 1919. Acceso al texto de la Sentencia en el siguiente enlace: https://supreme.justia.com/cases/federal/us/249/47/case.html

[78] El ejemplo fue enunciado por el juez Oliver Wendell Holmes al decir que sería gritar "¡Fuego!" en un cine lleno de gente. Estados Unidos. Tribunal Supremo. Caso Brandenburg vs Ohio. Sentencia de 8 de junio de 1969. Acceso al texto de la Sentencia en el siguiente enlace: https://supreme.justia.com/cases/federal/us/395/444/case.html

[79] Este caso se hizo famoso en la película *The People vs Larry Flynt*, traducida en España como "El escándalo de Larry Flynt". Estados Unidos. Tribunal Supremo. Caso Hustler Magazine vs. Falwell. Sentencia de 24 de febrero de 1988. Acceso al texto de la Sentencia en el siguiente enlace: https://supreme.justia.com/cases/federal/us/485/46/case.html

[80] Estados Unidos. Tribunal Supremo. Caso Garcetti vs. Ceballos. Sentencia de 30 de mayo de 2006. Acceso al texto de la Sentencia en el siguiente enlace: https://www.supremecourt.gov/Search.aspx?FileName=/docketfiles/04-473.htm

[81] La mayoría de las referencias jurisprudenciales se han recogido de MACOVEI, M., *Freedom of expression. A guide to the implementation of article 10 of the European Convention of Human Rights*, 2nd edition, Consejo de Europa, 2004, 65 p. Human Rights Handbook, nº 2. Constituye un sintético a la par que detallado compendio jurisprudencial sobre la materia.

Al igual que señalara el Tribunal Supremo en Estados Unidos, en Europea el TEDH ha dicho en repetidas ocasiones que la libertad de expresión constituye uno de los fundamentos esenciales de una sociedad democrática y una de las condiciones básicas para su progreso y para la realización de cada individuo (Sentencia *Lingens vs. Austria*[82], entre otras).

El artículo 10 reconoce tres proyecciones de la libertad de expresión: la libertad de opinión, que incluye el derecho a no ser obligado a manifestar la opinión (Sentencia *Vogt vs.* Alemania, 1995[83]); la libertad de difundir información e ideas, que incluye el derecho a criticar al gobierno (Sentencia *Lingens vs. Austria,* antes citada), el derecho a la libre expresión comercial, al igual que en Estados Unidos, (si bien es cierto que aquí el TEDH ha reconocido a las autoridades nacionales un mayor margen de apreciación; así en Sentencia *Markt Intern Verlag GmbH and Klaus Beermann vs. Alemania*, 1989[84]), y a la creación artística y su difusión (Sentencia *Otto-Preminger Institut vs. Austria*, 1994); y la libertad de recibir información, que conlleva tanto el derecho de los medios de comunicación a difundir información y opinión, como el derecho del público a estar bien informado.

Sin embargo, del mismo modo que hay un pronunciamiento claro respecto del reconocimiento y la consiguiente importancia de la libertad de expresión, en Europa la CEDH ha recogido expresamente límites en el propio artículo 10.2:"El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial".

Al igual que hemos visto en el derecho a la intimidad, en España, el reconocimiento de la libertad de expresión está igualmente plasmado en el texto constitucional. En concreto el

[82] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Pleno). Caso Lingens vs. Austria. Senencia de 8 de julio de 1986. Acceso al texto de la Sentencia en el siguiente enlace: http://hudoc.echr.coe.int/eng#{"dmdocnumber":["695400"],"itemid":["001-57523"]}
[83] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Pleno). Caso Vogt vs Alemania. Sentencia de 26 de septiembre de 1995.
[84] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Pleno). Caso Markt Intern Verlag GmbH and Klaus Beermann vs. Alemania. Sentencia de 20 de noviembre de 1989. Acceso al texto de la Sentencia en el siguiente enlace: http://freecases.eu/Doc/CourtAct/4555424

artículo 20.1 CE dice: “Se reconocen y protegen los derechos: a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción; b) A la producción y creación literaria, artística, científica y técnica; c) A la libertad de cátedra; y d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al ecreto profesional en el ejercicio de estas libertades”. De nuevo, *per se,* el citado artículo ya tiene un contenido. Sin embargo, al igual que acabamos de ver con la intimidad, y como no puede ser de otro modo ha existido una jurisprudencia constitucional que ha ido marcando en diferentes momentos, el contenido esencial de este derecho.

De manera aproximada y como elementos más relevantes podemos señalar cómo nuestro TC afirmó desde el principio que se trata de derechos de libertad frente al poder y comunes a todos los ciudadanos (así STC 6/1981[85]); que se trata de una libertad que cuyos límites son más amplios en función de las circunstancias, (STC 336/1993[86]), que además de un derecho fundamental es un valor objetivo esencial dentro de un Estado democrático (STC 85/1992[87]) y que contribuye a reconocer y garantizar una institución pública fundamental como es una opinión pública libre (STC 20/1990[88]).

Ahora bien, del mismo modo que el TEDH ha ido fijando los contornos del contenido de estos límites al ejercicio de la libertad de expresión, marcando claramente la necesidad de una interpretación estricta del clausulado al que hace referencia el citado art. 10.2 de la Convención (Sentencia *Sunday Times vs. Reino Unido*[89], 1979), cuestión esta sobre la que volveremos en otra parte de eta obra; también lo ha hecho nuestro Tribunal Constitucional al recordar que se trata de una libertad que no tiene un valor absoluto sino que debe

[85] España. Tribunal Constitucional (Sala Segunda). Sentencia 6/1981, de 16 de marzo. Acceso al texto de la Sentencia en el siguente enlace: http://hj.tribunalconstitucional.es/es/Resolucion/Show/6
[86] España. Tribunal Constitucional (Sala Segunda). Sentencia 336/1993, de 15 de noviembre. Acceso al texto de la Sentencia en el siguente enlace: http://ocw.usal.es/ciencias-sociales-1/derecho-a-la-informacion/contenidos/SENTENCIAS/2do%20BLOQUE/PDF/STC%20336-1993,%20de%2015%20de%20noviembre.pdf
[87] España. Tribunal Constitucional (Sala Segunda). Sentencia 85/1992, de 1 de julio. Acceso al texto de la Sentencia en el siguente enlace: http://hj.tribunalconstitucional.es/es/Resolucion/Show/1972
[88] España. Tribunal Constitucional (Sala Primera). Sentencia 20/1990, de 15 de febrero. Acceso al texto de la Sentencia en el siguente enlace: http://hj.tribunalconstitucional.es/gl/Resolucion/Show/1445
[89] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Pleno). Caso Sunday Times vs. Reino Unido. Sentencia de 26 de abril de 1979. Acceso al texto de la Sentencia en el siguiente enlace: http://hudoc.echr.coe.int/eng#{"dmdocnumber":["695461"],"itemid":["001-57584"]}

coordinarse con otros valores constitucionales cuando se producen entre ellos encuentros conflictivos (STC 241/1999[90]).

3.2 El derecho a la intimidad y la libertad de expresión como derechos de cuarta generación.

Vistas las características, sucintamente, del derecho a la intimidad y de la libertad de expresión en sentido clásico, lo que ahora corresponde, con base en el esquema anunciado, es ver en qué medida ambos derechos han visto modificado su contenido o cuáles son los problemas surgidos en la aplicación, reconocimiento y salvaguarda de estos derechos como consecuencia del surgimiento del desarrollo científico en general y de las nuevas tecnologías en particular. Como dijera muy gráficamente en su voto particular a la STC 290/2000 el Magistrado Jiménez de Parga, poniendo de manifiesto la importancia de estos dos derechos en el contexto tecnológico, "la denominada libertad informática, en cuanto derecho fundamental no recogido expresamente en el texto de 1978, debe tener como eje vertebrador el art. 10.1 CE, ya que es un derecho inherente a la dignidad de la persona. Tal vinculación a la dignidad de la persona proporciona a la libertad informática la debida consistencia constitucional. También son preceptos que facilitan la configuración de la libertad informática los contenidos en los arts. 18.1 (derecho al honor, a la intimidad personal y familiar y a la propia imagen) y 20.1 (libertad de expresión y de información), entre otros". Se trataba de una teoría, como luego veremos, destinada por el Magistrado a negar autonomía al derecho a la protección de datos.

3.2.1 El derecho a la intimidad como derecho de cuarta generación.

3.2.1.1 Una disquisición conceptual: intimidad, protección de datos y privacidad

Previamente a adentrarnos en los principales impactos sobre el derecho a la intimidad, es importante aportar una distinción de contenido respecto de otros conceptos como la libertad informática, el *habeas data* o el derecho a la protección de datos. Si llegáramos a la conclusión de que el derecho a la intimidad es equiparable al derecho a la protección de datos o que el derecho a la protección de datos es una consecuencia directa del derecho a

[90] España. Tribunal Constitucional (Sala Segunda). Sentencia 241/1999, de 20 de diciembre. Acceso al texto de la Sentencia en el siguente enlace: http://hj.tribunalconstitucional.es/es/Resolucion/Show/3983

la intimidad, el tratamiento de ambos por separado y la tesis que sostenemos respecto al contenido de la cuarta generación de derechos, carecería de sentido. El objetivo de este trabajo es atender a la validez del régimen jurídico actual de la protección de datos para la computación en nube, y ello exige saber y delimitar de qué estamos hablando. Y es que, como apunta Lucena Cid[91], "A pesar de la dificultad para definir y delimitar los espacios de la intimidad en nuestros días, la realidad nos impele a indagar un concepto que, si bien no pueda ser satisfactorio totalmente, sí tenga presente los nuevos desafíos que trae consigo el desarrollo de la informática y los avances de potentes sistemas tecnológicos cada vez más presentes en nuestra vida cotidiana". Por centrar el estudio y porque tiene un carácter instrumental, no se entra en disquisiciones sobre otros derechos muy vinculados a la intimidad como el derecho al honor, el derecho a la propia imagen o el derecho al secreto de las comunicaciones. No obstante muchas reflexiones sobre el derecho a la intimidad como derecho de cuarta generación serían perfectamente trasladables.

Más allá de lo conceptual, desde el punto de vista normativo, en Europa ya se fue consciente desde el principio de esta diferencia y buena prueba de ello es el Convenio 108 del Consejo de Europa antes citado que, en el precepto referido a las definiciones, habla de los datos de carácter personal referidos a cualquier información relativa a una persona física identificada o identificable (art. 2 a)). Se observa que se trata de cualquier información relativa a una persona con independencia de que afecte o no a la esfera íntima de la persona. De manera similar 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, en su Considerando 2, señala: "…sistemas de tratamiento de datos están al servicio del hombre; que deben,…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".

El texto de referencia en el ámbito del Consejo de Europa en materia de derechos fundamentales, la CEDH, no recoge, sin embargo, por razones cronológicas, esta distinción, aunque el Tribunal de Estrasburgo sí que ha aplicado el artículo 8 para dar lugar a un derecho

[91] Excelente trabajo sobre el concepto de intimidad, a pesar de que no compartamos algunas de sus afirmaciones particularmente en cuanto a la equiparación de privacidad/intimidad. LUCENA CID, I.V., La protección de la intimidad en la era teconlógica: hacia una reconceptualización, *Revista internacional de pensamiento político* [en línea], 2012, nº. 7, p. 117-144. Disponible en web: http://rabida.uhu.es/dspace/bitstream/handle/10272/7843/la_protecci%C3%B3n_de_la_intimidad.pdf?sequence=2 ISSN 1885-589X

a la protección de datos también así por ejemplo en la STEDH de 16 de febrero de 2000 (caso *Amann vs. Switzerland*)[92]. Si lo ha hecho de manera expresa, la citada Carta Europea de Derechos Fundamentales que trata en su artículo 7 la protección de la vida personal y familiar y contempla en el artículo 8 una referencia expresa al derecho a la protección de datos[93].

El legislador español también fue sensible a esta distinción desde el comienzo. Así, en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), la Exposición de motivos afirmaba que la privacidad era el bien jurídico protegido por la normativa de protección de datos, y lo diferenciaba de la intimidad[94]: "El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad: aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado.*"*

[92] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Gran Sala). Caso Amann vs. Switzerland. Sentencia de 16 de febrero de 2000.

[93] Artículo 7. Respeto a la vida privada y familiar
Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y del secreto de sus comunicaciones.
Artículo 8. Protección de datos de carácter personal
Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. Estos datos se tratarán de modo leal, para fines determinados 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 la conciernan y a su rectificación. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

[94] Es conocida la denominada «teoría del mosaico" que resulta sumamente gráfica: "datos objetivamente neutros, que no conculcan la intimidad, cruzados con otros de igual calificación, pueden dar lugar a una radiografía exacta del individuo que produzca distorsiones. Como dice Fernández Segado, "La informática se ha convertido así en un útil aliado del Estado por cuanto posibilita la transformación de informaciones dispersas en una información perfectamente organizada y sistematizada", en FERNÁNDEZ SEGADO, F., La dinamización de los mecanismos de garantía de los derechos y de los intereses difusos en el Estado social, ob. cit., p.

En la misma línea y siguiendo conceptualmente a la citada Exposición de Motivos, se pronunció el Tribunal Constitucional en su Sentencia 94/1998:[95] "el art. 18.4 …no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona -a la privacidad según el neologismo[96] que reza en la Exposición de Motivos de la LORTAD- pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos. Trata de evitar que la informatización de los datos personales propicie comportamientos discriminatorios".

La Ley Orgánica de Protección de Datos (LOPD) no fue tan explícita en esta diferenciación, pero sí que se deriva tanto de su art. 1 "La presente Ley Orgánica tiene por objeto 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 de su honor e intimidad personal y familiar*", como de su art. 3 a), en el que define los datos de carácter personal como "cualquier información concerniente a personas físicas identificadas o identificables", sin que por tanto tenga que afectar a la esfera íntima de la persona.

Como en todo lo relacionado con el Derecho de Internet, ha sido sin embargo la jurisprudencia la que más ha ayudado a la distinción. Como afirma Díaz Revorio, en este caso respecto al derecho a la protección de datos en España, lo que se ha producido es una evolución desde la idea inicial del texto constitucional que recogía un mandato al legislador; a una construcción jurisprudencial de un nuevo derecho fundamental, autónomo e independiente de otro[97]. En Europa la distinción entre uno y otro derecho se ha ido desarrollando, aunque de una manera matizada y gris, a lo largo de los últimos años[98]. Así,

---

[95] España. Tribunal Constitucional (Sala Segunda). Sentencia 94/1998, de 4 de mayo. Acceso al texto de la Sentencia en el siguiente enlace: http://hj.tribunalconstitucional.es/HJ/eu-ES/Resolucion/Show/SENTENCIA/1998/94

[96] El profesor Murillo de la Cueva habla de la palabra privacidad como un barbarismo; LUCAS MURILLO DE LA CUEVA, P., La construcción del derecho a la autodeterminación informativa, *Revista de estudios políticos*, 1999, nº 104, p. 47.
Bien es cierto que actualmente el Diccionario de la Real Academia de la Lengua (2010) admite dicha palabra y la define como: "Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión". Sobre el debate lingüístico ver DÍAZ ROJO, J.A., Privacidad: ¿neologismo o barbarismo?, *Espéculo, Revista de Estudios Literarios*, Julio-octubre 2002, nº 21. Disponible en Web: http://www.ucm.es/info/especulo/numero21/privaci.html, ISSN: 1139-3637

[97] DÍAZ REVORIO, F.J., ob. cit., p. 177 y 178.

[98] La mayoría de las referencias jurisprudenciales para abordar esta distinción en los tribunales europeos, tanto de Estrasburgo como de Luxemurgo, tomada de KOKOTT, J. y SOBOTTA, C., The distinction between privacy and data protection in the jurisprudence of the CJEU and the EctHR, *International Data Privacy Law*, 2013, vol. 3, nº. 4, p. 222-228.

el TJUE interpreta la jurisprudencia de Estrasburgo en cuanto al significado de "vida privada" como inclusivo de la protección de los datos personales, siendo definida como cualquier información relativa una persona identificada o identificable (STJUE, 9 de noviembre de 2010)[99]. Sin embargo, se debe introducir algún matiz, por cuanto el TEDH requiere algún elemento adicional de privacidad de cara a considerar la información personal como incluible en el ámbito de la vida privada, como por ejemplo que la información personal de que se trate se retrotraiga mucho en el tiempo y fuera recogida y almacenada sistemáticamente (STEDH, 4 de mayo de 2000)[100]. De ello, Kokott y Sobotta[101] se plantean si se podría deducir a contrario que una recopilación y almacenamiento de datos personales menos sistemática, no afectaría a la vida privada bajo el sistema de Estrasburgo. Esta postura, añadimos, confirmaría el diferente ámbito de aplicación de uno y otro derecho.

La jurisprudencia de Estrasburgo, en los casos *Amann vs. Switzerland* y *Rotaru vs Romania* ya citados, ha señalado por tanto que la recogida, almacenamiento y revelación de información concerniente a la vida privada interfiere con el derecho a la intimidad; sin perjuicio de que dicha injerencia, como señala el artículo 8.2 CEDH, es posible siempre que 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 de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás; unos límites por cierto más específicos que los del artículo 52.1 CDFUE de permitir las injerencias 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.

Por tanto, una primera distinción en el ámbito de la jurisprudencia derivada de los textos europeos es la referida al ámbito de cada uno de los derechos porque la información cubierta por el derecho a la intimidad y el derecho a la protección de datos, no es el mismo. La vida privada no incluye necesariamente toda la información de una persona identificada o identificable; y sin embargo la protección de datos cubre precisamente dicha información[102].

---

[99] Unión Europea.Tribunal de Justicia de la Unión Europea. Casos Volker und Markus Schecke GbR (C-92/09) y Hartmut Eifert (C-93/09) vs. Land Hessen. Sentencia de 9 de noviembre de 2012. Acceso al texto de la Sentencia en el siguiente enlace:

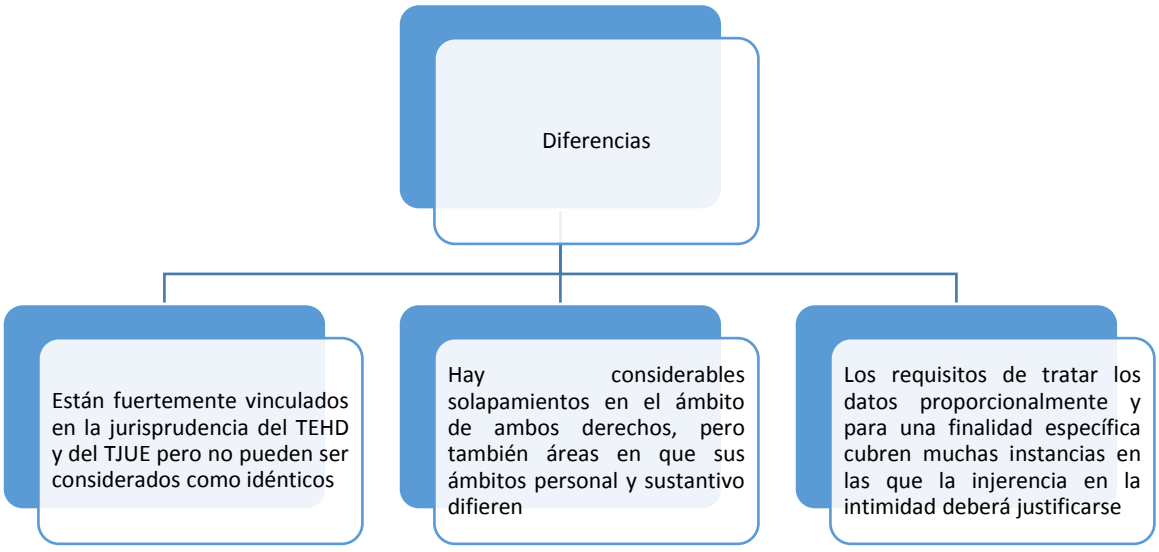
[100] Consejo de Europa.Tribunal Europeo de Derechos Humanos. Caso Rotaru v Romania. Sentencia de 4 de mayo de 2000. Acceso al texto de la Sentencia en el siguiente enlace: http://hudoc.echr.coe.int/eng#{"itemid":["001-58586"]}

[101] El primero Abogado General el TJUE y el segundo Secretario Jurídico (*Legal Secretary*).

[102] KOKOTT, J. y SOBOTTA, C, ob. cit., p. 225.

Igualmente, la jurisprudencia ha distinguido en cuanto al ámbito personal, por cuanto el TJUE ha excluido a las personas jurídicas de la protección de datos (STJUE de 9 de noviembre de 2000 antes citada), que sin embargo sí son titulares del derecho a la intimidad (STEDH de 8 de julio de 2013)[103]. Otra distinción derivada de la jurisprudencia radica en las injerencias permitidas y es que recordemos que el artículo 8 CDFUE señala que los datos se tratarán de modo leal, para fines determinados y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Pero no podemos olvidar que, si bien cuando concurran estas circunstancias no se verá vulnerado el derecho a la protección de datos, las Sentencias de los citados casos *Amann vs. Switzerland* y *Rotaru vs Romania* han señalado que la recogida, almacenamiento y revelación de dichos datos podría todavía afectar a la vida privada y exigiría por tanto justificación desde la perspectiva de este acuerdo

A modo de conclusión, y siguiendo a los citados Kokott y Sobottta, podemos resumir la relación entre uno y otro derecho del siguiente modo[104]:



Fuente: elaboración propia

[103] Consejo de Europa.Tribunal Europeo de Derechos Humanos (Sección Primera). Caso bernh Larsen Holding AS and others v Norway App. Sentencia de 8 de julio de 2013.
[104] KOKOTT, J. y SOBOTTA, C, ob. cit., p. 228.

En la misma línea, e incluso se puede decir que con una mayor rotundidad y claridad, el Tribunal Constitucional español, en el Fundamento Jurídico 6 de su Sentencia 292/2000[105], en la que se pronunció sobre determinados preceptos de la LOPD, acabó de fijar las principales diferencias entre el derecho a la intimidad y el derecho a la protección de datos: "De ahí la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como *esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada*, *inextricablemente unidos al respeto de la dignidad personal*[106] …como el derecho al honor, citado expresamente en el art. 18.4 CE, e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona ….el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal".

Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido[107], ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido…el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales.

La sustantividad propia de cada uno de los dos derechos ha sido acogida igualmente por las autoridades públicas, y así la Agencia Española de Protección de Datos subraya que "puede informar sobre el derecho a la protección de datos de carácter personal, también llamado de

[105] España. Tribunal Constitucional (Pleno). Sentencia núm. 292/2000 de 30 de noviembre.
[106] La cursiva es nuestra
[107] La Enciclopedia Jurídica Omeba es muy clara cuando dice que "Todo lo íntimo es necesariamente privado, pero no todo lo privado es necesariamente íntimo".

autodeterminación informativa por el Tribunal Constitucional, y no sobre el derecho a la intimidad y a la propia imagen"[108].

En el plano doctrinal también se ha marcado esta diferencia al señalar que el bien jurídico al que se refiere el artículo 18.4 no se refiere solamente a la reserva personal y familiar, sino también a los derechos, libertades y garantías fundamentales de los ciudadanos. Como dice el profesor Aspas, "la autodeterminación informativa como derecho fundamental autónomo guarda relación de complementariedad con otros derechos y libertades fundamentales…"[109]. Sobre la segunda vertiente aportada por el Tribunal Constitucional se pronuncia Megías Quirós, quien recuerda que "este derecho fundamental (referido al art. 18.4) aporta – a la vertiente negativa, de exclusión, de la intimidad – una vertiente positiva que lo diferencia notablemente de la intimidad…e insiste al afirmar que hay que distinguir netamente entre la facultad de excluir del conocimiento de los datos y la de controlarlos"[110]. Cierto es que este autor va más allá al sostener que el derecho a la intimidad tiene un carácter material, frente al secreto de las comunicaciones, la inviolabilidad del domicilio o el control de determinados datos, que tienen un carácter más formal destinado a evitar que se llegue al contenido de la intimidad[111]. De similar modo, Villaverde Menéndez recuerda que "justamente el objeto de protección del derecho fundamental es el dato ya conocido, bien porque se ha consentido su conocimiento por terceros, o bien porque una norma así lo dispone. El dato ha salido de la esfera privada del sujeto, y se trata ahora de establecer en qué condiciones su tráfico, su circulación es constitucionalmente adecuada"[112]. Por último, el profesor Fernández Segado sintetiza esta diferenciación cuando dice que la libertad informática ya no es un derecho a la intimidad entendida como separación y defensa de la sociedad; es un nuevo derecho social de libertad, no es ya únicamente el derecho a negar la información sobre sí mismo, sino también el derecho a pretenderla[113].

Todas estas afirmaciones, líneas grises y contornos borrosos, no son sino una consecuencia de que, como afirma Fernández Rodríguez "la problemática de la protección de datos es una

[108] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Informe 0077/2013.
[109] ASPAS ASPAS, J.M., ob. cit. p. 364
[110] MEGÍAS QUIRÓS, J.J., Privacidad e internet: intimidad, comunicaciones y datos personales, *Anuario de derechos humanos*, 2002, nº. 3, p. 519 y 530.
[111] *idem,* p. 524.
[112] VILLAVERDE MENÉNDEZ, I., Nuevas tecnologías, videovigilancia, derecho a la protección de datos y ficheros policiales, *Revista Catalana de Seguridad Pública,* 2006, nº 16, p. 180. Disponible en web: http://www.raco.cat/index.php/rcsp/article/viewFile/130221/179659
[113] FERNÁNDEZ SEGADO, F., La dinamización de los mecanismos de garantía de los derechos y de los intereses difusos en el Estado social, ob. cit.

más de las que nacen de la interacción entre informática e intimidad"[114]. Y es que como recuerda García Mexía la noción de privacidad engloba toda una serie de conceptos aledaños como el de intimidad, el de confidencialidad, el de protección de datos como derecho, la noción de seguridad y la noción de identidad digital[115]. De manera similar, pero inversa en cuanto al uso de los términos intimidad y privacidad, Pérez Luño afirma que la pluralidad de manifestaciones en las que la intimidad se manifiesta (privacidad/privacy, datos personales, perfil de personalidad, autodeterminación informativa...) no implican una disolución del concepto unitario de intimidad, sino más bien su ampliación y adaptación a las exigencias de un mundo en cambio[116].

En todo caso la dificultad conceptual no es patrimonio único de nuestra doctrina y así en la doctrina americana, más allá de la evolución jurisprudencial que ya hemos visto, son muchos los conceptos que se han vinculado o con los que se ha definido la privacidad *(privacy*)[117]: el derecho a que te dejen en paz, en la clásica formulación de Warren y Brandeis; el acceso limitado a uno mismo: la habilidad de blindar a uno mismo del acceso no querido por parte de otros; el secretismo: el encubrimiento de ciertas materias de otros; el control sobre la información personal y la habilidad de ejercer control sobre la información de uno mismo; personalidad: la protección de la personalidad de uno, de la individualidad y de la dignidad; y la intimidad *(intimacy)*: control sobre o acceso limitado a las relaciones íntimas de unos u otros aspectos de la vida.

En definitiva, se trata de una distinción no siempre sencilla y buena prueba de ello es que uno de los grandes expertos sobre la materia, el profesor Piñar Mañas, habla, al hilo de los arts. 7 y 8 CDFUE, de derecho a la privacidad (mientras que nosotros lo hemos identificado como derecho a la intimidad propiamente dicho) y de derecho a la protección de datos (enmarcado a nuestro juicio en el derecho a la privacidad) respectivamente[118].

Como conclusión, y como reflejamos en la siguiente figura, a nuestro juicio, el derecho a la privacidad en sentido estricto es el derecho que engloba tanto al derecho a la intimidad en

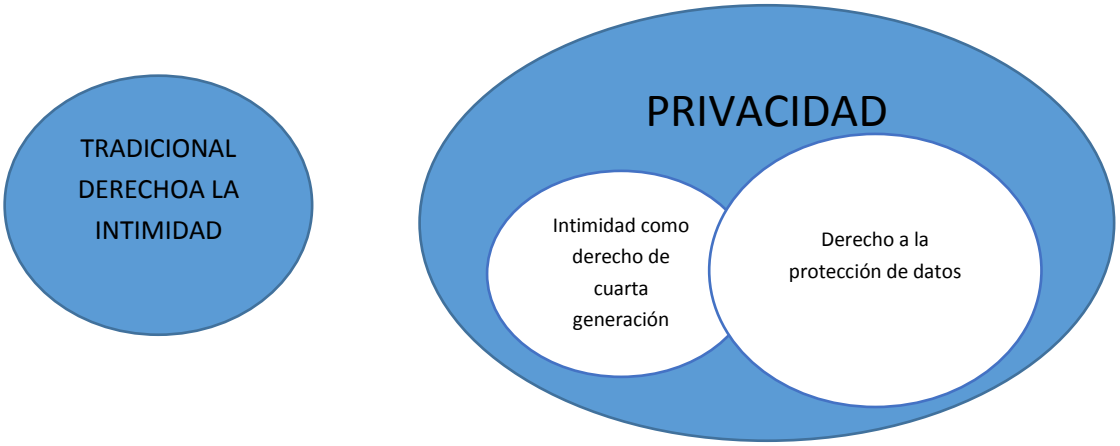
---

[114] FERNÁNDEZ RODRÍGUEZ, J.J., *Lo público y lo privado en Internet. Intimidad y libertad de expresión en la Red*, Instituto de Investigaciones Jurídica, Universidad Nacional Autónoma de México, 2004. p. 95.
[115] GARCÍA MEXÍA, P.L., *Derechos y libertades, internet y tics*, Valencia, Tirant lo Blanch, p. 22-24, internet y tic's.
[116] PÉREZ LUÑO, A.E., Bioética e intimidad. La tutela de los datos personales biomédicos, en *Bioética y derechos humanos*, Ana María Marcos del Cano (coord..), Universidad Nacional de Educación a Distancia, 2011, p. 77-104.
[117] SOLOVE, D.J., Conceptualizing Privacy, *California Law Review,* 2002, vol. 90, issue 4, article 2, p. 1087-1155. Disponible en web: http://scholarship.law.berkeley.edu/californialawreview/vol90/iss4/2
[118] LUCAS MURILLO DE LA CUEVA, P., y PIÑAR MAÑAS, J.L., ob. cit., p 94.

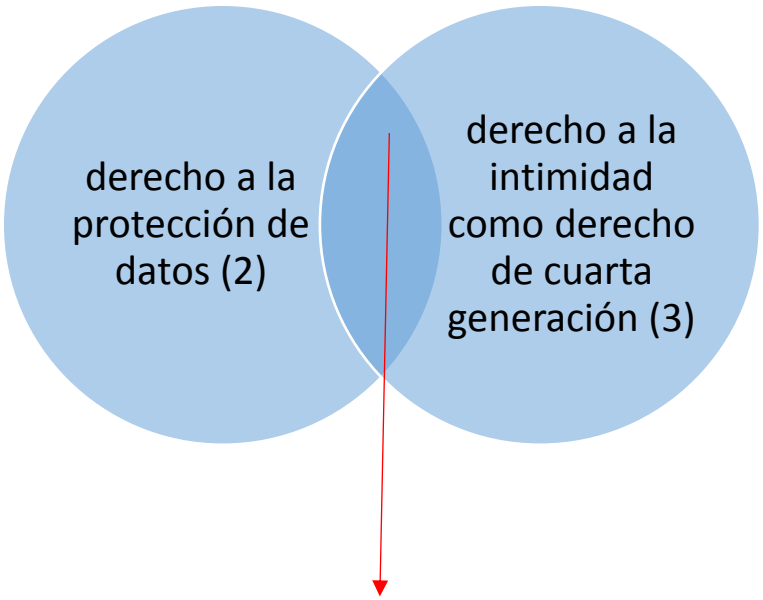
cuanto que derecho de cuarta generación, es decir, en cuanto que derecho afectado por la evolución científica y tecnológica, como el derecho a la protección de datos personales. Ello sin perjuicio de que en determinadas ocasiones estos dos últimos tienen una interconexión instrumental en el sentido apuntado por la jurisprudencia europea antes citada, esto es, en el sentido de que en determinadas ocasiones la quiebra del derecho fundamental a la protección de datos puede dar lugar a la vulneración del derecho a la intimidad. Sin embargo, como vamos a ver, la afectación del derecho a la intimidad como derecho de cuarta generación se puede dar por vías distintas de la protección de datos propiamente dicha y consiguientemente goza, reiteramos, de una sustantividad propia.

En conclusión, podemos tener una intimidad vulnerada por una quiebra del derecho a la protección de datos (1), podemos tener una quiebra de la protección de datos sin que se vea vulnerado el derecho a la intimidad (2) y podemos tener un derecho a la intimidad vulnerado por la tecnología sin que sea consecuencia de una vulneración del derecho a la protección de datos, al menos con dimensión constitucional (3), si bien es cierto que este último supuesto está cuestionado, en gran medida como consecuencia de que el concepto de dato personal ha alcanzado tal amplitud que es difícil encontrar algo vinculado a la persona que no entre dentro de dicha categoría. En realidad, estamos en una postura muy similar a la que ya sostuviera la STC de 20 de julio de 1993[119]: “nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de 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”.

[119] España. Tribunal Constitucional (Sala Primera). Sentencia núm. 254/1993, de 20 de julio.



CONTENIDO DE LA PRIVACIDAD



Derecho a la intimidad como derecho de cuarta generación consecuencia de la vulneración del derecho fundamental a la protección de datos (1)

Nota: en el concepto de privacidad se incluirían también derechos como el derecho al secreto de las comunicaciones, el derecho al honor o el derecho a la propia imagen en cuanto que afectados por el fenómeno tecnológico

Fuente: elaboración propia

3.2.1.2 Tecnología y derecho a la intimidad

Hecha esta distinción conceptual y de contenido entre el derecho a la intimidad y la libertad informática o el derecho a la autodeterminación informativa, nos corresponde, ahora sí,

adentrarnos en el impacto que las nuevas tecnologías han tenido en el derecho a la intimidad propiamente dicho. Algunas reflexiones que veremos resultarán también útiles con posterioridad para dar respuesta –en línea con el objetivo último de este trabajo– a si el régimen jurídico actual resulta válido para el entorno de la computación en nube.

Internet ha afectado de manera profunda a la intimidad de las personas, incluso provocando una absoluta indefensión en el usuario de Internet[120]. No olvidemos que los primeros argumentos de Warren y Brandeis para la protección jurídica de la privacidad estuvieron en gran parte motivados por la expansión de las tecnologías de la comunicación tales como el desarrollo de los periódicos de gran difusión o la multiplicación de las reproducciones impresas de fotografías. Del mismo modo la protección de la Cuarta Enmienda contra registros y confiscaciones se amplió posteriormente en el siglo XX para proteger frente a las escuchas telefónicas y la vigilancia electrónica[121]. Como expuso Philip Zimmermann en su informe ante el Subcomité de Política Económica, Comercio y Medio Ambiente del Congreso de los EE.UU, "en el pasado, cuando el Estado pretendía violar la intimidad de los ciudadanos debía esforzarse en interceptar, abrir al vapor y leer el correo. Era como pescar con caña, de pieza en pieza. Los mensajes de correo electrónico son más fáciles de interceptar y se pueden escanear a gran escala, y ordenar en función de palabras claves. Esto es como pescar con red, y supone una diferencia orwelliana cuantitativa y cualitativa para la garantía de la democracia"[122]. Es curioso que este tipo de símiles con los tradicionales medios de comunicación han sido también utilizado por la jurisprudencia. Así en Sentencia del Tribunal Superior Regional de Colonia, este afirmaba que el envío de un correo electrónico a "solo una o dos personas determinadas" equivaldría al envío de una carta, cuyo contenido sólo puede ser visto por sus específicos destinatarios; por el contrario, el envío de un correo electrónico a más de dos personas se asemejaría al de una tarjeta postal, cuyo contenido puede ser abiertamente leído por terceros y que por ene difícilmente puede ser considerado privado por su remitente[123].

Como hemos apuntado, no es baladí ni casual que la denominada libertad informática en la Constitución española se encuentre recogida en el mismo artículo en el que lo está el

---

[120] VERA SANTOS, J.M., Derechos fundamentales, Internet y nuevas tecnologías; en GARCÍA MEXÍA, P. (coord), *Principios de Derecho de Internet*, ob. cit., p. 195.
[121] AA.VV *"Privacy*", en *Stanford Enciclopedia of Philosoph*y.
[122] PÉREZ LUÑO, A.E., Impactos sociales y jurídicos de Internet, *Argumentos de razón técnica: Revista española de ciencia, tecnología y sociedad, y filosofía de la tecnología* [en línea], 1998, Nº 1, p. 33-48. Disponible en Web: http://www.argumentos.us.es/numero1/bluno.htm ISSN 1139-3327
[123] Cita tomada de GARCÍA MEXÍA, P.L, *Derecho Europeo de Internet*, ob. cit., p. 88.

derecho a la intimidad o al secreto de las comunicaciones. El derecho a la intimidad está especialmente afectado por las nuevas tecnologías[124] y constituye sin lugar a dudas, más allá de la sustantividad del derecho a la protección de datos, el derecho más amenazado. Esta visión no resulta algo reciente, sino que se remonta en el plano oficial al año 1968 cuando la Asamblea Parlamentaria de Naciones Unidas recomendó al Consejo de Ministros estudiar los peligros que el uso de los equipos tecnológicos y científicos representaba para los derechos humanos.

En el plano doctrinal por su parte, como dice el profesor Pérez Luño, "Internet implica….el riesgo de un efecto multiplicador de los atentados contra derechos, bienes e intereses jurídicos. Su potencialidad en la difusión ilimitada de imágenes e informaciones la hace un vehículo especialmente poderoso para perpetrar atentados criminales contra bienes jurídicos básicos: la intimidad…."[125]. Pero además, por otro lado, incide el mismo profesor, "Para combatir las nuevas formas de criminalidad potenciadas a través de la Red, se han creado potentes sistemas estatales de seguridad….Estos sistemas entrañan, sin embargo, un preocupante riesgo para las libertades cívicas, al suponer implacables mecanismos de control social y de perforación de la intimidad" [126]. En similar sentido, Maud de Boer-Buquicchio afirma que los dos grandes retos de Internet, que además se encuentran conectados, son la confianza en Internet y el derecho a la intimidad[127].

La realidad es que hoy día muchas de las tecnologías, y fundamentalmente la navegación en Internet, pueden suponer un grave riesgo para el derecho a la intimidad. Siguiendo a Fernández Rodríguez, podemos señalar los siguientes comportamientos que pueden atentar contra la intimidad[128]: la entrada en el disco duro del ordenador sin consentimiento, la

---

[124] Vamos a seguir manteniendo el vocablo de derecho a la intimidad a pesar de que hay autores que han hablado de que, como consecuencia del impacto de las nuevas tecnologías, ya no basta con hablar de intimidad, sino que, en línea con lo que hemos ido viendo en el cuerpo del texto, hay que hablar de privacidad, que constituiría un conjunto más amplio de facetas de la personalidad que el individuo tiene derecho a mantener reservadas. DE CARRERAS SERRA, LL., *Régimen jurídico de la Información. Periodistas y Medios de Comunicación*, Ariel Derecho, 1996, p. 71, y FERNÁNDEZ ESTEBAN, M.L., El impacto de las nuevas tecnologías e Internet en los derechos del art. 18 de la Constitución, *Anuario de la Facultad de Derecho, Universidad de Extremadura*, 1999, nº 17, p. 523 a 544. Tal y como hemos reflejado, el término privacidad tendría un contenido más amplio.

[125] PEREZ LUÑO, A.E, Internet y los derechos humanos, *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento* [en línea], 2002, nº 2, Facultad de Derecho, Universidad de Huelva, p. 101-121, Disponible en web: http://www.uhu.es/derechoyconocimiento/DyC02/DYC002_A05.pdf ISSN 1578-8202.

[126] *Idem*, p. 107

[127] DE BOER-BUQUICCHIO, M.,*Conférence sur l'éthique et les droits de l'homme dans la société de l'information*, Consejo de Europa, Estrasburgo, 13 de septiembre de 2007.

[128] FERNÁNDEZ RODRÍGUEZ, J.J., ob. cit., p. 99 y 100.

interceptación de mensajes de correo electrónico y de las comunicaciones en general, la suplantación de identidad de un usuario o de la identidad de una computadora, el hostigamiento electrónico, el uso indebido de directorios de correo electrónico o de listas de usuarios, la alteración o destrucción de información o el acceso a la cuenta del administrador. Bien es cierto que el profesor Fernández Rodríguez incluye también otros comportamientos que, a mi juicio, inciden de manera más directa en la privacidad que en la intimidad propiamente dicha: la elaboración de perfiles del navegante con fines publicitarios u otros más graves, la simple acumulación o registro de datos sin consentimiento; la transferencia de datos sin consentimiento, el empleo de una dirección IP asignada a otro ordenador o el impedimento para acceder a la información (interrupción del servicio). Y es que coincidimos con Pérez Ugena al señalar que la conexión entre intimidad e informática plantea una serie de cuestiones que no pueden resolverse acudiendo a un análisis de la LOPD[129], a pesar de que ciertamente existe una corriente de lo que Ricard Martínez ha denominado el poder de atracción del derecho fundamental a la protección de datos[130].

En este sentido, y siguiendo el esquema que hemos defendió, sea como consecuencia de una afectación tecnológica directa, sea como consecuencia de un tratamiento de datos que afectan a la esfera íntima de la persona, el derecho a la intimidad se ha situado en primera línea en cuanto al impacto que ha supuesto en su configuración el desarrollo tecnológico. A título de ejemplo, como refleja Nissenbaum una teoría de la intimidad (usa el término *privacy*) en público nunca se ha desarrollado completamente porque hasta el advenimiento de la tecnología moderna nunca había sido un problema[131]. Nuestro Tribunal Constitucional, ya en Sentencia 110/1984 [132] , de 26 de noviembre, recordaba que "el avance de la tecnología actual y el desarrollo de los medios de comunicación de masas ha obligado a extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad y del respeto a la correspondencia, que es o puede ser medio de conocimiento de aspectos de la vida privada. De aquí el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por

[129] PÉREZ-UGENA, A. y PÉREZ UGENA, M.P., Implicaciones constitucionales de las nuevas tecnologías, *Revista de Derecho Político*, 2002, nº 54, p.153-195, Disponible en web: http://e-spacio.uned.es/fez/eserv/bibliuned:DerechoPolitico-2002-54-10021/PDF

[130] MARTÍNEZ MARTÍNEZ, R., El derecho fundamental a la protección de datos: perspectivas, *IDP: revista de Internet, derecho y política = revista d'Internet, dret i política* [en línea], 2007, nº 5. Disponible en web: http://www.uoc.edu/idp/5/dt/esp/martinez.pdf, ISSN-e 1699-8154.

[131] NISSENBAUM, H., Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*, 1998, vol. 17, p. 559-596. Disponible en web: https://pdfs.semanticscholar.org/307f/83f933ae0c4e53392b7c0046d3dc24e2e4f3.pdf

[132] España. Tribunal Constitucional (Sección Tercera). Sentencia 110/1984, de 26 de noviembre.

cualquier medio puedan realizarse en ese ámbito reservado de vida. No siempre es fácil, sin embargo, acotar con nitidez el contenido de la intimidad", y en la Sentencia 119/2001, de 24 de mayo, añadía que "habida cuenta de que nuestro texto constitucional no consagra derechos meramente teóricos o ilusorios, sino reales y efectivos …, se hace imprescindible asegurar su protección no sólo frente a las injerencias ya mencionadas, sino también frente a los riesgos que puedan surgir en una sociedad tecnológicamente avanzada"[133]. En el plano doctrinal, subraya Guissasola Lerma que "el galopante avance de las nuevas tecnologías ha conducido a un replanteamiento del derecho a la intimidad"[134] y en otras latitudes, el profesor Reidenberg señala que la transparencia de la información personal habilitada a través de tecnologías online sofisticadas socava el significado y valor de las tradicionales doctrinas constitucionales americanas sobre la privacidad (intimidad)[135].

Hay dos ámbitos concretos en los que el impacto de la tecnología en el derecho a la intimidad ha sido particularmente acusado: el de la investigación por el Estado y el de las relaciones laborales.

Sin perjuicio de lo que se verá en otro capítulo de esta obra al hilo del acceso a la información por parte de las autoridades públicas en los entornos de computación en nube, en su dimensión constitucional, un ámbito de particular incidencia para el derecho a la intimidad ha sido el de las investigaciones policiales y judiciales y el acceso a dispositivos informáticos. Como apunta Schwartzberg cuando se usa la tecnología para descubrir pruebas de robo de identidad, transacciones de droga o pornografía infantil, los tribunales se enfrentan a la aplicación de salvaguardas legales y constitucionales para proteger al individuo en este entorno cambiante[136]. En el plano jurisprudencial lo podemos ver en la muy relevante STC 173/2011, de 7 de noviembre[137]. Se trataba de un caso donde se dirimía, en el seno de una investigación criminal, si tanto en el acceso al ordenador por parte del dueño de la tienda donde llevó a repararlo, como por parte de los policías nacionales que accedieron al ordenador sin previa autorización judicial, se vulneraba el derecho a la intimidad. Se planteaba el Tribunal si un ordenador personal puede ser un medio idóneo para el ejercicio

[133] España. Tribunal Constitucional (Pleno). Sentencia 119/2001, de 24 de mayo. Acceso al texto de la Sentencia en el siguiente enlace: http://hj.tribunalconstitucional.es/ca/Resolucion/Show/4415
[134] GUISSASOLA LERMA, C., Menores, intimidad y riesgos de la Sociedad tecnológica: el caso particular del sexting, en FAYOS GARDÓ, A., (Coord.), *Los derechos a la intimidad y a la privacidad en el siglo XXI,* Dykinson, 2015, p. 114
[135] REIDENBERT, J.R., Privacy in Public, *University of Miami Law Review,* 2014, vol. 69, p. 141-160.
[136] SCHWARTZBERG, S., Hacking the fourth: how the gaps in the law and fourth amendment jurisprudence leave the right to privacy at risk, *University of La Verne Law Review*¸ abril 2009, vol. 30, p. 467-494.
[137] España. Tribunal Constitucional (Sala Segunda). Sentencia 173/2011, de 7 de noviembre.

de la intimidad personal, y afirmaba con rotundidad que "está dentro del ámbito de la intimidad constitucionalmente protegido,…el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) —por lo que sus funciones podrían equipararse a los de una agenda electrónica—, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc.". Y añadía igualmente, mostrando de nuevo la íntima conexión de todos los derechos del artículo 18, que "…el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado".

En similares planteamientos y también en el campo de las investigaciones policiales y penales, se pronunciaba el TC en su Sentencia 142/2012, de 2 de julio[138], respecto al acceso por parte de la Guardia Civil a la agenda del teléfono móvil de una persona coimputada, y a la potencial vulneración del derecho a la intimidad y del derecho al secreto de las comunicaciones, que en este caso sin embargo no fue apreciada. Precisamente en referencia a los teléfonos móviles, el Tribunal Constitucional, en Sentencia 115/2013, de 9 de mayo[139], ha señalado que "la versatilidad tecnológica que han alcanzado los teléfonos móviles convierte a estos terminales en herramientas indispensables en la vida cotidiana con múltiples funciones, tanto de recopilación y almacenamiento de datos como de comunicación con terceros (llamadas de voz, grabación de voz, mensajes de texto, acceso a internet y comunicación con terceros a través de internet, archivos con fotos, videos, etc.), susceptibles, según los diferentes supuestos a considerar en cada caso, de afectar no sólo

[138] España. Tribunal Constitucional (Sala Primera). Sentencia 142/2012, de 2 de julio.
[139] España. Tribunal Constitucional (Pleno). Sentencia 115/2013, de 9 de mayo.

al derecho al secreto de las comunicaciones (art. 18.3 CE), sino también a los derechos al honor, a la intimidad personal y a la propia imagen (art. 18.1 CE), e incluso al derecho a la protección de datos personales (art. 18.4 CE), lo que implica que el parámetro de control a proyectar sobre la conducta de acceso a dicho instrumento deba ser especialmente riguroso, tanto desde la perspectiva de la existencia de norma legal habilitante, incluyendo la necesaria calidad de la ley, como desde la perspectiva de si la concreta actuación desarrollada al amparo de la ley se ha ejecutado respetando escrupulosamente el principio de proporcionalidad".

En el plano doctrinal se puede ver también esta múltiple afectación a los derechos del artículo 18, y así señala Delgado Martín[140] que el acceso a la información contenida en los dispositivos electrónicos (teléfonos móviles, «Smartphones», tabletas, ordenadores, dispositivos USB, ZIP, CDOROM, DVD, reproductores de MP3 o MP4, servidores de Información, entre otros), por parte del sistema penal puede afectar a varios derechos fundamentales: a la intimidad personal, al secreto de las comunicaciones e incluso al derecho a la autodeterminación informativa en el ámbito de la protección de datos personales.

Fuera de nuestras fronteras, esta cuestión también se ha planteado en diversas jurisdicciones. Resulta muy significativa por ejemplo la doctrina sentada por el Tribunal Supremo de Canadá donde se pone de manifiesto el particular impacto de la tecnología y de los dispositivos tecnológicos en la intimidad de la persona, y que refuerza sin duda nuestra tesis de que la realidad tecnológica ha alterado sustancialmente el contenido de dicho derecho, a pesar de que se sostenga en los mismos principios. Así, en su Sentencia de 7 de noviembre de 2013[141], afirmaba rotundamente que "es difícil imaginar una invasión más intrusiva de la privacidad que la búsqueda en un ordenador personal", y en línea con lo visto en nuestra jurisprudencia, extendía dicha reflexión a los teléfonos móviles al afirmar que "no distingo, a los efectos de una autorización previa, los ordenadores de los teléfonos móviles. A pesar de que históricamente los teléfonos móviles estaban mucho más limitados que los ordenadores en términos de cantidad y tipo de información que pudieran almacenar, hoy día los teléfonos tienen capacidades que son, a nuestros efectos, equivalentes a los de dichos

[140] DELGADO MARTÍN, J., Derechos fundamentales afectados en el acceso al contenido de dispositivos electrónicos para la investigación de delitos, *Diario La Ley*, 29 de noviembre de 2013 nº 8202, Sección Doctrina.
[141] Canadá. Tribunal Supremo. Caso R. *v.* Vu. Sentencia de 7 de noviembre de 2013. Acceso al texto de la Sentencia en el siguiente enlace: http://www.canlii.org/en/ca/scc/doc/2013/2013scc60/2013scc60.html?searchUrlHash=AAAAAQALMjAxMyBTQ0MgNjAAAAAAAQ

ordenadores". Pero mayor importancia si cabe tiene, a los efectos de nuestra argumentación, del impacto exponencial de la tecnología en el derecho a la intimidad, su descripción de las características que hacen de los ordenadores (trasladémoslo a cualquier otro dispositivo tecnológico) esencialmente diferentes de recipientes físicos encontrados en unas instalaciones: "los ordenadores almacenan una ingente cantidad de información, que es previsible afecte "el núcleo biográfico de información personal", los ordenadores contienen información que se genera automáticamente, a menudo sin conocimiento del usuario, un archivo de ordenador y otros datos permanecerán en un ordenador incluso después de que el usuario crea que se han borrado, y un ordenador puede permitir la búsqueda de un punto que no esté "físicamente presente" en las instalaciones si el ordenador está conectado a Internet, permitiendo así la búsqueda o registro que abarca un ámbito mucho mayor que el tradicional registro de unas instalaciones[142].

Precisamente en Estados Unidos la posibilidad de acceso al contenido de los teléfonos móviles de una persona detenida por parte de las autoridades policiales sin necesidad de una orden de registro provocó en los últimos años una amplia polémica. A la misma puso fin la Sentencia del Tribunal Supremo exigiendo a la policía la correspondiente orden judicial en el famoso caso *Ridley vs. California* de 25 de junio de 2014[143], en la que entre otras afirmaciones señaló que los teléfonos inteligentes y otros dispositivos electrónicos no están en la misma categoría que las carteras, los maletines y los vehículos; y remataba muy gráficamente que "sería como considerar que montar a caballo es lo mismo que un vuelo a la luna".

Y terminaba con una frase digna de mención: "los modernos teléfonos móviles no son simplemente otra utilidad tecnológica. Con todo lo que contienen y todo lo que pueden revelar, albergan para la mayoría de los americanos "las intimidades de su vida" (*the privacies of life*). Respecto a esta decisión, el Director de la Unión Americana para las Libertades Civiles, en coincidencia con lo que se defiende en estas líneas, señaló que "mediante el reconocimiento de que la revolución digital ha transformado nuestras

[142] BANKS, T., Supreme Court of Canada to Police: Get a Warrant to Search Computers and Mobile Phones [en línea], *Privacy and Cybersecurity Law*, 8 de noviembre de 2013. Disponible en web: http://www.privacyandcybersecuritylaw.com/supreme-court-of-canada-to-police-geWall t-a-warrant-to-search-computers-and-mobile-phones

[143] Estados Unidos. Tribunal Supremo. Caso Ridley vs. California. Sentencia de 25 de junio de 2014. Acceso al texto de la Sentencia en el siguiente enlace: https://supreme.justia.com/cases/federal/us/573/13-132/case.pdf

expectativas de privacidad, la decisión de hoy es en sí misma revolucionaria y ayudará a proteger los derechos a la intimidad (*Privacy rights*) de todos los americanos"[144].

Pero incluso cabe señalar que esta problemática de la potencial vulneración del derecho a la intimidad fruto del acceso a la información en dispositivos electrónicos se ha dado también en el ámbito civil, y así se puede observar en el caso resuelto por la Corte de Apelación del Quinto Distrito del Estado de Florida en un caso[145] de divorcio en el que la esposa instaló un *spyware* para controlar la conducta de su marido y descubrió que había estado comunicándose con otra mujer. La evidencia obtenida por la mujer utilizando dicho programa informático se anuló por considerarlo una invasión de la intimidad y fue considerada como un registro abusivo. A pesar de que la tecnología *spyware* era utilizada por el público en general, el marido tenía una expectativa subjetiva de privacidad en sus comunicaciones en línea. En fin, las infinitas posibilidades de la tecnología han planteado numerosos debates como por ejemplo la legalidad o no de la utilización de un dispositivo de imágenes térmicas desde la calle para detectar la presencia de droga en el garaje de un domicilio[146], o el debate abierto en Estados Unidos respecto al uso de drones en la seguridad interior y sus implicaciones para el derecho a la intimidad[147].

En numerosas ocasiones, fruto del supuesto en que el derecho a la protección de datos tiene una naturaleza de garantía o de instrumento de defensa de la intimidad de la persona, se consideran conculcados expresamente ambos derechos. Así ocurrió por ejemplo en la STC 202/1999 de 16 de diciembre[148], en la que se suscitaba la conformidad con el art. 18 CE del tratamiento y conservación en el preciso soporte informático de los datos atinentes a la salud del trabajador…prescindiendo del consentimiento expreso del afectado, y en el que se declaraba expresamente que conculcaba el derecho a la intimidad y a la

[144] BRAVIN, J., Supreme Court: Police Need Warrants to Search Cellphone Data, *Wall Street Journal*, 25 de junio de 2014. Disponible en Web: http://www.wsj.com/articles/high-court-police-usually-need-warrants-for-cell-phone-data-1403706571

[145] Estados Unidos. Corte de Apelación del Quinto Distrito del Estado de Florida. Sentencia de 11 de febrero de 2005. Acceso al texto de la Sentencia en el siguiente enlace: http://www.divorcereality.com/wp-content/uploads/2015/01/OBrien-case2.pdf

[146] Estados Unidos. Sentencia de la Corte de Apelación del Noveno Distrito Federal. Sentencia de 11 de junio de 2001. Acceso al texto de la Sentencia en el siguiente enlace: https://supreme.justia.com/cases/federal/us/533/27/case.pdf

[147] MATITEYAHU, T., Drone Regulations and Fourth Amendment Rights: The Interaction of State Drone Statutes and the Reasonable Expectation of Privacy, *Columbia Journal of Law and Social Problems*, Winter2015, Vol. 48 Issue 2, p. 265-307. Disponible en web: http://www.columbia.edu/cu/jlsp/pdf/Spring2015/Matiteyahu.pdf. En la misma línea, THOMPSON, R.M., Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses, *Congressional Research Service*, 2013. Disponible en web: https://fas.org/sgp/crs/natsec/R42701.pdf

[148] España. Tribunal Constitucional (Sala Primera). Sentencia 202/1999 de 16 de diciembre.

libertad informática del titular de la información. En esta íntima relación entre ambos derechos, pero reconociendo la sustantividad específica de cada uno de ellos, merece subrayarse en el ámbito de la genética, la argumentación del Ministerio Fiscal[149] recogida en la STC 135/2014, de 8 de septiembre, en la que se afirmaba que "la diligencia de la obtención de una muestra de saliva al recurrente, para su posterior análisis de los perfiles genéticos, afecta a la intimidad personal (art. 18.1 CE), en su manifestación como intimidad genética, no por la forma en que ésta se practica (frotis bucal), que en sí misma no supone una injerencia intolerable en la intimidad corporal del mismo, sino por su finalidad, esto es, por el tipo de información que puede obtenerse de dicha prueba. Por ello, la obtención de una muestra biológica del cuerpo de una persona para el posterior análisis de los perfiles identificadores de ADN del afectado quedaría amparada por el derecho a la intimidad personal (art. 18.1 CE). Por su parte, la conservación de las muestras biológicas, así como de los perfiles identificadores de ADN, y su almacenamiento, custodia y eventuales usos futuros quedaría amparada por el derecho a la protección de datos personales o autodeterminación informativa (art. 18.4 CE)". En la misma línea cronológica parece situarse Delgado Martín en el campo de las investigaciones policiales y del acceso a la información a dispositivos electrónicos al situar la entrada en juego del derecho a la protección de datos en el tratamiento posterior de la información del dispositivo electrónico afectado[150].

Más allá de las investigaciones policiales y la afectación que las mismas pueden tener respecto a la intimidad cuando se interconectan con dispositivos tecnológicos, otro ámbito en el que estos han tenido un particular impacto en el referido derecho ha sido el de las relaciones laborales. Ello, sin perjuicio de los supuestos, algunos de los cuales mencionaremos, en los que se ha dilucidado también la concurrencia de este derecho con el derecho fundamental a la protección de datos, y prueba de ello también en el plano pseudo normativo ha sido que la Agencia Española de Protección de Datos le ha dedicado una guía específica a la materia[151] o el Código elaborado por la Organización Internacional del Trabajo

[149] En referencia a la importancia de la relación entre tecnología y delito, así como en la importancia del uso de las tenologías para la investigación de los mismos, ver el Informe del Informe del Consejo Fiscal al Anteproyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas. Disponible en web: http://pdfs.wke.es/2/2/7/8/pd0000102278.pdf

[150] DELGADO MARTÍN, J., ob. cit.

[151] España. Agencia Española de Protección de Datos. Guía de Relaciones Laborales. 2009. Disponible en web: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_RelacionesLaborales2.pdf

respecto a la protección de datos en el trabajo[152]. En todo caso, como afirma Ortiz de Solórzano Aurusa, la problemática derivada del uso de las nuevas tecnologías en la relación laboral es amplia y cambiante, abarcando desde el teletrabajo, a las relaciones colectivas -el denominado sindicalismo en línea- pasando por el uso de las TICs en el puesto de trabajo[153]. Por no hablar de fenómenos vinculados a la cuarta revolución industrial por la interacción que se está dando entre ellos: inteligencia artificial y el aprendizaje automático, la robótica, la nanotecnología las impresoras 3D y la genética y la biotecnología[154]. No obstante, nos vamos a centrar exclusivamente en el conflicto entre el poder de control del empresario y el derecho a la intimidad del trabajador en su afectación por el uso de la tecnología.

Desde un punto de vista institucional, estas cuestiones se trataron tempranamente, y así, en la Unión Europea, el Grupo de Trabajo del artículo 29 sentó en 2002 los criterios respecto a la protección de la intimidad de los trabajadores en el uso de las comunicaciones electrónicas[155]. En concreto se pueden señalar las siguientes reglas[156]: los trabajadores tienen una expectativa legítima de privacidad en su puesto de trabajo, que no se ve desplazada por el hecho de usar dispositivos de los empleadores, sin perjuicio de que la provisión de una adecuada información por parte de los empleadores a los trabajadores puede reducir su legítima expectativa de privacidad; el principio general de secreto que informa la correspondencia cubre las comunicaciones en el trabajo, incluyendo los correos electrónicos y los archivos adjuntos; el respeto a la vida privada incluye también un cierto grado de derecho a establecer y desarrollar las relaciones con otros seres humanos, y el

[152] INTERNATIONAL LABOUR ORGANIZATION. Protection of workers' personal data. 1997. Disponible en web: http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf

[153] ORTIZ DE SOLÓRZANO AURUSA, C., Facultades empresariales de control, tics y privacidad del trabajador, *Revista Aranzadi de derecho y nuevas tecnologías*, 2015, nº 37, p. 41-72. Esta autora distingue precisamente en este artículo la afectación en el derecho a la intimidad y en el derecho a la protección de datos personales.

[154] WORLD ECONOMIC FORUM, *The Future of Jobs Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution*, January 2016. Disponible en web: http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf

[155] GRUPO DE TRABAJO DEL ARTÍCULO 29, Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo, (WP 55), 2002. Disponible en web: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_es.pdf

[156] LASPROGATA, G., KING, N., y PILLAY, S., Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada, *Stanford Techonology Law Review*, 2004, nº 4. Disponbible en web: http://weblife.io/wp-content/uploads/2013/09/Lasprogata-RegulationElectronic.pdf

hecho de que dichas relaciones, en gran medida, tengan lugar en el puesto de trabajo, impone límites a la necesidad legítima de medidas de vigilancia por parte del empleador.

En los planos doctrinal y jurisprudencial, también son muchos los pronunciamientos en los que se han dilucidado estas cuestiones. Los conflictos han sido abundantes porque, como señalan Fernández Avilés y Rodríguez-Rico, "el desarrollo de las nuevas tecnologías se ha visto acompañado en el tiempo de un paralelo proceso de centralidad del derecho a la intimidad del trabajador, conforme se asumía el riesgo que generan aquéllas en la protección de este derecho"[157]. Y es que estamos ante un incremento no meramente cuantitativo, sino cualitativo, de las facultades de control del empresario gracias a estas tecnologías[158], fruto de que, como dice Segoviano Astaburuaga, "a través de las nuevas tecnologías el empleador pasa a controlar, no sólo la actividad productiva, sino también la persona del trabajador"[159]; en gran medida porque se han difuminado lo que antes eran unas fronteras claras entre las vidas profesional y personal del trabajador[160].

La doctrina extranjera tampoco ha sido ajena a esta realidad. Así, Wallach señala que es difícil imaginar un lugar de trabajo hoy día en el que no se utilicen los medios digitales, esto es, el uso de ordenadores (Internet y correo electrónico), teléfonos móviles (y teléfonos fijos) y todo tipo de equipos de vigilancia y monitorización como por ejemplos circuitos cerrados de televisión y todo tipo de cámaras. Y añade que hoy día es posible con un coste mínimo y normalmente utilizando dispositivos ya instalados en el lugar de trabajo, tales como ordenadores y teléfonos, llevara a cabo una labor de vigilancia y control de las actividades de los empleados como sus actividades, su nivel de atención, con quién se comunican y los contenidos de sus comunicaciones, incluyendo Internet y los correos electrónicos"[161]. Y como concluye Marta Otto, "este acceso sin precedentes a la esfera personal de los empleados

---

[157] FERNÁNDEZ AVILÉS, J.A. y RODRÍGUEZ-RICO ROLDÁN, V., Nuevas tecnologías y control empresarial de la actividad laboral es España [en línea], *Labour&Law Issues* 2016*,* vol. 2, nº 1.

[158] CARDONA RUBERT, M.B., Las relaciones laborales y el uso de las tecnologías informáticas [en línea], *Lan harremanak: Revista de relaciones laborales*, 2003, nº Extra 1, p. 157-173. En la misma línea de ese cambio cualitativo y no solamente de grado, y dentro de la doctrina extranjera, LEVINSON, A.R., Industrial Justice: Privacy Protection for the Employed, *Cornell Journal of Law and Public Policy,* 2009, vol 18, p. 609-688. Disponible en web: http://scholarship.law.cornell.edu/cjlpp/vol18/iss3/1

[159] SEGOVIANO ASTABURUAGA, M.L., El difícil equilibrio entre el poder de dirección del empresario y los derechos fundamentales de los trabajadores [en línea], *Revista jurídica de Castilla y León*, 2004, nº 2, p. 147-190. ISSN 1696-6759. En la misma línea y con una afirmación prácticamente idéntica, GUDE FERNÁNDEZ, A., La videovigilancia laboral y el derecho a la protección de datos de carácter personal, *Revista de derecho político*, 2014, nº 91, p. 43-90.

[160] LASPROGATA, G., KING, N., y PILLAY, S., ob. cit.

[161] WALLACH, S., The Medusa Stare: Surveillance and Monitoring of Employees and the Right to Privacy, *International Journal of Comparative Labour Law and Industrial Relations*, 2011, p. 189-219.

añade indiscutiblemente una nueva dimensión al problema fundamental de acomodo razonable de intereses aparentemente contradictorios, particularmente el poder de dirección del empresario y la intimidad del trabajador"[162].

Como en ocasiones anteriores y más allá de las reflexiones doctrinales, ha sido la jurisprudencia, muy abundante en la materia, la que ha ido marcando las pautas. A nivel europeo, merece destacarse la STEDH de 3 de abril de 2007 (*Copland vs. United Kingdom*)[163] en la que, a la hora de fijar el ámbito de actuación del derecho a la intimidad señalaba que "de acuerdo con la jurisprudencia el Tribunal, las llamadas de teléfono desde el puesto de trabajo están en principio cubiertas por la noción de "vida privada" …Y resulta lógico por tanto que los correos electrónicos enviados desde el trabajo estén igualmente protegidos por el artículo 8, al igual que la información derivada de la vigilancia del uso personal de Internet". Considerando que el recurrente en ese caso no había sido avisado de que podría estar sometido a control, tenía una expectativa razonable de privacidad respecto a las llamadas que hacía desde el teléfono de su trabajo. La misma expectativa debería aplicarse en relación a los correos electrónicos y a la navegación por Internet.

En la misma línea de la existencia o no de avisos, esto es, de normas claras fijadas por el empresario respecto al uso de los medios electrónicos; así como del adecuado equilibrio entre el empresario y el trabajador, se puede observar la STEDH de 12 de enero de 2016 (caso *Barbulescu vs. Rumania*)[164]. Se trataba de un supuesto en el que el ingeniero responsable de ventas de una empresa, creó una cuenta de Yahoo Messenger para atender las solicitudes de los clientes. El empleador, tras comprobar que la cuenta de correo se había usado para fines particulares, despidió al trabajador, basándose en que la regulación interna de la empresa prohibía expresamente la utilización de ordenadores, teléfonos, fax y demás medios para fines personales. El TEDH señaló que se había controlado el correo del trabajador suponiendo que solo contenía comunicaciones derivadas de su trabajo y que ni siquiera se accedió al contenido de las mismas, sino que simplemente dicho control se hizo en el marco de un procedimiento disciplinario, para verificar si verdaderamente el trabajador

[162] OTTO, M., *The Right to Privacy in Employment: A Comparative Analysis,* Bloomsbury Publishing, 2016, 256 p.
[163] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Sección Cuarta). Copland vs. United Kingdom Sentencia de 7 de abril de 2000.
[164] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Sección Cuarta). Caso Barbulescu vs. Rumania. Sentencia de 12 de enero de 2016.

utilizó el ordenador de la empresa con fines distintos a los estrictamente laborales durante la jornada de trabajo.

En nuestro país, en el caso de la jurisprudencia ordinaria hay que detenerse en tres sentencias: la STS 6128/2007 de 26 de septiembre[165], en la que básicamente se dilucidaba si los controles empresariales sobre los ordenadores facilitados a los trabajadores por la empresa eran o no compatibles con el derecho a la intimidad que le reconoce al trabajador el Estatuto de los Trabajadores. En dicha Sentencia reconduce el debate al poder de vigilancia y control del empresario previsto en el art. 20.3 del Estatuto de los Trabajadores pero añadiendo dos matizaciones: la primera remite a un ejercicio de las facultades de vigilancia y control que guarde "en su adopción y aplicación la consideración debida" a la dignidad del trabajador, lo que también remite a su vez al respeto a la intimidad; y la segunda se refiere al alcance de la protección de la intimidad que es compatible con el control lícito. Esta doctrina se resume a nuestro juicio en las siguientes palabras: "…la existencia de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos…facilitados por la empresa a los trabajadores. Esa tolerancia crea una expectativa también general de confidencialidad en esos usos; …que no puede ser desconocida, aunque tampoco convertirse en un impedimento permanente del control empresarial, …lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios…e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos. De esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado "una expectativa razonable de intimidad".

Esta doctrina fue reiterada en STS 1630/2011 de 8 de marzo[166], y sin embargo llevada más allá en la STS 8876/2011, de 6 de octubre, por cuanto nuestro TS señaló, tras reconocer que se puede imponer una prohibición absoluta de uso personal de medios informáticos, afirmaba que: "si no hay derecho a utilizar el ordenador para usos personales, no habrá tampoco derecho para hacerlo en unas condiciones que impongan un respeto a la intimidad o al secreto de las comunicaciones, porque, al no existir una situación de tolerancia del uso

[165] España. Tribunal Supremo (Sala de lo Social, Sección 1ª). Sentencia núm. 6128/2007 de 26 de septiembre.
[166] España. Tribunal Supremo (Sala de lo Social, Sección 1ª). Sentencia núm. 1630/2011 de 8 de marzo.

personal, tampoco existe ya una expectativa razonable de intimidad y porque, si el uso personal es ilícito, no puede exigirse al empresario que lo soporte y que además se abstenga de controlarlo". En definitiva, en esta Sentencia, de similar modo que ha hecho el caso Barbulescu antes citado, se consagró la posibilidad de anular el derecho a la intimidad del trabajador en el uso de los dispositivos informáticos o, en palabras del propio TS: "En el caso del uso personal de los medios informáticos de la empresa no puede existir un conflicto de derechos cuando hay una prohibición válida". Cabe subrayar respecto a esta afirmación, el voto particular de la Magistrada Segoviano Astaburuaga, y al que se adhirieron otros cuatro Magistrados, en el que señalaba que "…para que la empresa pueda proceder al control del uso del ordenador por parte del trabajador, sin vulnerar su "expectativa de confidencialidad" y, por ende, su dignidad, no solo ha de haber establecido instrucciones para su uso, sino también advertido de los controles que van a aplicarse. No es suficiente con que el empresario establezca válidamente una prohibición absoluta de uso de medios de la empresa (ordenadores, móviles, internet, etc...) para fines propios, tanto dentro como fuera del horario de trabajo sino que, además ha de advertir de los controles que se van a utilizar para conocer el uso del ordenador por parte del trabajador".

Cono no podía ser de otro modo, el conflicto también ha llegado a nuestro Tribunal Constitucional. En este sentido cabe partir, para fijar el ámbito del adecuado equilibrio, por un lado de la doctrina que marca, entre muchas otras, la STC de 19 de julio de 1985[167] respecto a que el contrato de trabajo no puede considerarse como un título legitimador de recortes en el ejercicio de los derechos fundamentales que incumben al trabajador como ciudadano, que no pierde su condición de tal por insertarse en el ámbito de una organización privada; y por otro la sentada por la STC de 17 de diciembre de 2012[168], en cuanto a que no cabe duda de que es admisible la ordenación y regulación del uso de los medios informáticos de titularidad empresarial por parte del trabajador, así como la facultad empresarial de vigilancia y control del cumplimiento de las obligaciones relativas a la utilización del medio en cuestión, siempre con pleno respeto a los derechos fundamentales.

Sentadas estas premisas, y en línea con lo debatido por el TS, merece la pena detenerse en la STC de 7 de octubre de 2013[169], por cuanto goza, como afirma el propio TC (de nuevo poniendo de manifiesto la novedad), de trascendencia constitucional, por no existir, en el

[167] España. Tribunal Constitucional (Sala Primera). Sentencia 88/1985 de 19 de julio.
[168] España. Tribunal Constitucional (Sala Primera). Sentencia 241/2012 de 7 de diciembre.
[169] España. Tribunal Constitucional (Sala Primera). Sentencia 170/2013 de 7 de octubre.

momento de admisión a trámite, doctrina constitucional sobre el alcance de los derechos a la intimidad y secreto de las comunicaciones en el ámbito laboral en relación con los correos electrónicos. Se trataba de un supuesto en el que la empresa había accedido al contenido de los correos electrónicos del trabajador registrados en el ordenador de la entidad y que permitió acceder a mensajes relativos a la transmisión a terceros de información empresarial reservada por parte del trabajador. El TC consideró que no se vio vulnerado el derecho a la intimidad. En concreto, en lo que concierne al control del uso del ordenador, afirmaba que "la habilitación por la empresa de esta herramienta informática como medio para llevar a cabo el adecuado cumplimiento de la prestación de trabajo y el hecho de que su uso para fines distintos de los relacionados con el contenido de la prestación laboral estuviera tipificado en el Convenio colectivo aplicable como infracción sancionable impiden considerar que su utilización quedara al margen del control empresarial". Y además, en una doctrina ya consolidada en cuanto a la limitación del derecho a la intimidad, en lo que concierne al acceso al contenido de los correos electrónicos del trabajador para verificar que se había facilitado información confidencial de la empresa, se sometió al juicio de proporcionalidad, es decir, se constató que cumplía con las tres condiciones que conforman dicho juicio: "si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)".

Precisamente este último mecanismo de verificación de la constitucionalidad o no de una medida, había sido aplicado por nuestro TC en las primeras Sentencias sobre audiovigilancia y videovigilancia en el trabajo (Sentencias de 10 de abril[170] y de 10 de julio de 2000[171] respectivamente), y además con fallos opuestos. Tradicionalmente por tanto el sometimiento del trabajador a este tipo de vigilancias había sido confrontado con su derecho a la intimidad. Más recientemente, demostrando la consolidación de esta doctrina, el TC en su Sentencia de 3 de marzo de 2016[172] consideró que la instalación de una cámara de videovigilancia en la tienda donde prestaba sus servicios la demandante para controlar la caja donde trabajaba al haberse detectado irregularidades dinerarias no vulneró el derecho a la intimidad al haber

[170] España. Tribunal Constitucional (Sala Primera). Sentencia 98/2000, de 10 de abril.
[171] España. Tribunal Constitucional (Sala Primera). Sentencia 186/2000, de 10 de julio.
[172] España. Tribunal Constitucional (Pleno). Sentencia 39/2016, de 3 de marzo.

superado el juicio de proporcionalidad, toda vez que existían sospechas razonables de ciertas irregularidades y la grabación de imágenes se limitó a la zona de caja.

Fuera de nuestras fronteras, la línea jurisprudencial es muy parecida. Así, en Francia[173], una de las primeras sentencias sobre esta materia fue la dictada por la Corte de Casación el 2 de octubre de 2001 en el caso *Nikon France vs. Onof*[174], que marcó una doctrina particularmente protectora de la intimida del trabajador. En la misma se decía que trabajadores tiene un derecho a la vida privada en su lugar de trabajo, incluyendo el derecho a la intimidad de su correspondencia personal en los sistemas del empresario; y añadía que "el empleador no puede violar este derecho fundamental leyendo los mensajes enviados o recibidos por el trabajador a través de un dispositivo del trabajo, incluso si la compañía ha prohibido el uso personal de los ordenadores". Sin embargo, esta doctrina se ha visto años después matizada,. Así, el mismo tribunal, en su Sentencia de 15 de diciembre de 2009[175], en el caso *Bruno B vs. Giraud et Migot*, introdujo un mayor equilibrio. Se trataba de una empresa de auditoria que despidió a un trabajador tras haber descubierto unos archivos en su ordenador de trabajo y enviados a autoridades gubernamentales, en los que menospreciaba a la empresa por supuestos fraudes fiscales así como por las condiciones laborales. El trabajador alegó la violación de su intimidad porque los documentos eran datos personales. La Corte dio la razón a la empresa porque al no haber marcado el trabajador sus documentos como "privados", estaba justificado que la compañía asumiera que dichos documentos estaban relacionados con el trabajo y consiguientemente podía abrirlos. Esta doctrina que exige de una actitud proactiva del trabajador a la hora de marcar sus documentos como privados fue ratificada por la Corte de Casación en su Sentencia de 19 de diciembre de 2013[176].

En el caso italiano[177], destacamos por un lado la Sentencia del Tribunal de Casación de 19 de diciembre de 2007[178] en la que se decía que el empleador que lee los correos electrónicos de sus trabajadores no viola el secreto de la correspondencia si se tiene en cuenta que

[173] Comentarios y descripción de casos tomadas parcialmente de KAMBELLARI, E., Employee email monitoring and workplace privacy in the European perspective, *Iustinianus Primus Law Review*, 2014, nº 8, p. 1-18 y LINDSAY, A.F., y JEFFERIES, T.R., *French court limits the scope of employee data protection*, 2013. Disponible en web: http://www.lexology.com/library/detail.aspx?g=0b1abe79-8a71-4625-b43a-f40b58c27673
[174] Francia. Corte de Casación. Caso Nikon France vs. Onof. Sentencia de 2 de octubre de 2001.
[175] Francia. Corte de Casación. Caso Bruno B v. Giraud et Migot. Sentencia 15 de diciembre de 2009.
[176] Francia. Corte de Casación. Caso Monsieur X v. Young & Rubicam Franc. Sentencia de 19 de diciembre de 2013.
[177] KAMBELLARI, E., ob. cit., p. 14.
[178] Italia. Tribunal de Casación. Sentencia de 19 de diciembre de 2007.

previamente la empresa había fijado una norma bajo la cual el trabajador tenía que facilitar al empleador las contraseñas de su ordenador y de su correo electrónico. De nuevo en una manifestación de la búsqueda de equilibrio, merece igualmente destacarse la Sentencia del Tribunal de Distrito de Turín de 20 de agosto de 2006[179] en la que señalaba que el correo electrónico pertenece al empleador y que cualquier acto por el que se tenga conocimiento sobre el contenido de los correos electrónicos de los trabajadores no constituye una vulneración del secreto de la correspondencia, pero añade, y aquí es donde se pone de manifiesto el equilibrio, el único requisito que se debe cumplir por parte del empleador es asegurar que dicha actuación vaya precedida de una política empresarial específica.

Mención aparte merece el caso de los Estados Unidos, donde, al igual que en los ámbitos comunitario y español, no hay propiamente una regulación de esta cuestión en el ámbito laboral. Sí que podemos citar que la Ley de Intimidad de las Comunicaciones Electrónicas (*Electronic Communications Privacy Act,* ECPA) considera ilícito en general la lectura o divulgación de los contenidos de una comunicación electrónica, aunque contempla numerosas excepciones: los PSI pueden ver correos privados si sospechan que su emisor está intentando dañar el sistema o a otro usuario, aunque un control aleatorio del correo electrónico está prohibido; también pueden ver o divulgar legalmente correos privados si el emisor o el receptor del mensaje consienten su visión o divulgación; si el correo electrónico es propiedad del empleador, el empleador puede inspeccionar los contenidos del sistema de correo electrónico de sus empleados, por lo que un correo enviado desde el lugar de negocio probablemente no es privado, cuestión esta sobre la que ahora veremos el tratamiento jurisprudencial; los servidores pueden ser obligados a divulgar información personal en respuesta a una orden o citación judicial, si bien es cierto que para obtener información básica del suscriptor basta una citación, aunque para obtener un mayor grado de información las autoridades norteamericanas necesitan de una orden de registro; y particular mención hay que hacer a la *USA PATRIOT Act*[180], que ha hecho más fácil para el gobierno acceder a los registros de la actividad en línea, ya que, en un esfuerzo para aumentar la velocidad en que se accede a los registros, la Ley elimina gran parte de la supervisión a cargo de otras ramas del gobierno y amplía los tipos de registros que pueden solicitarse sin una orden

[179] Italia. Tribunal de Distrito de Turín. Sentencia de 20 de agosto de 2006.
[180] *USA PATRIOT* responde al acrónimo de *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (Unir y fortalecer América facilitando herramientas apropiadas requeridas para interceptar y obstaculizar los actos terroristas de 2001). Acceso al texto de la norma en el siguiente enlace: https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

judicial; sin perjuicio de que se ha visto a su vez muy matizada y limitada por la aprobación en junio de 2015 de la *USA Freedom Act*.

En el ámbito específicamente laboral, y ante la ausencia de una regulación específica, es necesario acudir a las resoluciones judiciales para ver las líneas de actuación que han de seguir los trabajadores y el grado de intimidad de que gozan en su puesto de trabajo en lo concerniente al uso del correo electrónico. En general, con base en la ECPA antes citada, el trabajador no dispone de privacidad respecto del empleador cuando se trata de la utilización de los medios aportados por la empresa, sin perjuicio de que alguna Sentencia como la dictada por el Tribunal del Noveno Circuito Judicial de 18 de junio de 2008[181] en el caso *Quon v. Arch Wireless Operating Co.*, ha planteado la posibilidad de uso de algunas de las cláusulas de la ECPA para la protección de los trabajadores[182].

No obstante, la mayoritaria postura de los tribunales americanos *Gina M Holmes vs. Petrovich Development Company* (Sentencia de la Corte de Apelación de California de 13 de enero de 2011)[183] consideró como no confidenciales los correos electrónicos entre la demandante y su abogado con base en los siguientes criterios: porque utilizó un ordenador de la compañía demandada para mandar correos electrónicos a pesar de conocer la política de la compañía respecto a que el ordenador solo se debía utilizar para los negocios de la

[181] Los Tribunales de Circuito son los Tribunales de "segunda instancia" en algunos Estados, como ocurre en este caso en el Estado de California.
Estados Unidos. Tribunal del Noveno Circuito Judicial. caso Quon v. Arch Wireless Operating Co. Sentencia de 18 de junio de 2008. Acceso al texto de la Sentencia en el siguiente enlace: http://caselaw.findlaw.com/us-9th-circuit/1144813.html

[182] Ver en este sentido el artículo de LEVNISON, A.R., Toward a cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees, *West Virginia Law Review*, vol. 114 2011, p. 461-550. Disponible en web: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1798822, donde hace un análisis de las posibilidades de uso de la ECPA y de la *Stored Communications Act* para la defensa de la intimidad de los trabajadores hasta tanto no se proceda a una reforma en dicho sentido. La Sentencia se puede leer en http://epic.org/privacy/workplace/9th_cir_quon.pdf. Se trataba del caso del Departamento de Policía de Ontario que decidió contratar con un proveedor (la empresa demandada) el sistema de buscas y de mensajes de texto. El teniente al cargo del sistema permitía a los policías la utilización del sistema de mensajes de texto para usos personales siempre y cuando fuera pagado por ellos cuando superasen un determinado volumen. Las dificultades de cobro conllevaron que un superior interviniera en la cuestión solicitando al proveedor del servicio una copia de los mensajes, entre otros del demandado, algo a lo que procedió el citado proveedor. El Tribunal revocó la decisión del Juzgado que había dictado la primera sentencia al considerar que no cabía dar copia de dichos mensajes al empleador si previamente no habí obtenido el consentimiento del trabajador con base en que dicho proceder violaba las prescripciones de la ECPA.

[183] Estados Unidos. Corte de Apelación de California. Gina M Holmes vs. Petrovich Development Company. Sentencia de 13 de enero de 2011. Para ver un resumen de la Sentencia http://www.leagle.com/xmlResult.aspx?xmldoc=In%20CACO%2020110113032.xml&docbase=CSLWAR3-2007-CURR
Para ver la Sentencia completa, http://lawyersusaonline.com/wp-files/pdfs-2/holmes-v-petrovich-development.pdf

compañía y que tenían prohibido su uso para enviar o recibir correos personales; fue avisada de que la empresa vigilaría sus ordenadores para verificar el cumplimiento de esta política y así podría inspeccionar todos los archivos y mensajes en cualquier momento; y fue expresamente avisada de que los trabajadores no tendrían ninguna "expectativa de privacidad" respecto de la información o mensajes personales remitidos o recibidos en los ordenadores de la compañía.

A pesar de este pronunciamiento, cabe establecer algunas matizaciones. Así en el caso *Stengart vs. Loving Care Agency*, cuya Sentencia fue dictada por el Tribunal Supremo de New Jersey el 30 de marzo de 2010[184], el Tribunal reconocía la expectativa de privacidad de una trabajadora respecto de su cuenta de correo personal y protegida bajo una contraseña, con independencia de que se haya utilizado un ordenador propiedad de la empresa. Bien es cierto que en este caso el Tribunal contaba con el argumento reforzado de la confidencialidad derivada de la relación abogado-cliente, puesto que se trataba de correos electrónicos intercambiados entre la trabajadora y su abogado, lo cual estrecha el margen del precedente, máxime si, como apuntan algunos comentarios a la Sentencia, la política de la empresa de utilización de las comunicaciones electrónicas no era clara[185].

También es digna de mención la particular trascendencia que adquiere la condición de empleado público o de empleado de una compañía privada a efectos de ver garantizada tu intimidad respecto al poder de control del empresario. Efectivamente, como sentara la Sentencia *O'Connor vs. Ortega*[186], la Cuarta Enmienda, referida al derecho a la intimidad o a la privacidad como ya hemos visto, solamente resulta aplicable respecto de la monitorización o control gubernamental, lo que llevaba a que los empleados públicos tenían un grado superior de protección de su intimidad que los empleados privados. Además de la polémica en si misma de dicha doctrina, adoptada por un ajustado 5-4 y con la figura de la *plurality opinion*, fue posteriormente matizada en la Sentencia *City of Ontario vs. Qohn*[187], en

[184] Estados Unidos. Tribunal Supremo de New Jersey. caso Stengart v. Loving Care Agency. Sentencia de 30 de marzo de 2010. Acceso al texto de a Sentencia en el siguiente enlace: http://caselaw.findlaw.com/nj-supreme-court/1522648.html

[185] COSSROW. B.A, The Fig Leaf Precedent Set by *Stengart v. Loving Care Agency Inc*, *Technology Law, Bloomberg Law Repports*, 2010, vol 2, nº 10. Disponible en web: http://www.laborlawyers.com/files/25559_the%20fig%20leaf%20precedent%20set%20by%20ste.pdf

[186] Estados Unidos. Tribunal Supremo. Caso City of Ontario vs. Qohn. Sentencia de 31 de marzo de 1987. Acceso al texto de la Sentencia en el siguiente enlace: https://supreme.justia.com/cases/federal/us/480/709/case.html

[187] Estados Unidos. Tribunal Supremo. caso Stengart v. Loving Care Agency. Sentencia de 19 de abril de 2010. Acceso al texto de la Sentencia en el siguiente enlace: https://www.supremecourt.gov/opinions/09pdf/08-1332.pdf

la que culminó uno de los casos anteriormente citados, y que además estaba referida expresamente al acceso a las comunicaciones electrónicas (en concreto, un bíper de un policía) donde señaló que en este caso el acceso estaba relacionado con el trabajo y consiguientemente no vulneraba la cuarta enmienda. A ello cabe añadir que en la realidad la diferencia entre los empleados públicos y los empleados privados no es tal por varios motivos: el control por parte del empleador de las instalaciones y de los equipamientos, el consentimiento implícito del trabajador que está generalmente informado respecto de la posibilidad de vigilancia por parte del empleador, y el equilibrio en cuanto a la magnitud de la invasión del poder de control del empleador en la intimidad o información personal frente a las necesidades del negocio y la eficiencia del empleado público, todo ello combinado conlleva una gran limitación de la razonable expectativa de privacidad del empleado público[188].

3.2.2 El derecho a la libertad de expresión como derecho de cuarta generación.

3.2.2.1 Breve referencia al principio de neutralidad

El siguiente derecho que podemos observar que está cualitativamente afectado por Internet es la libertad de expresión. John Barlow, uno de los fundadores de la *Electronic Frontier Foundation* y autor de la Declaración de Independencia del Ciberespacio, afirmaba rotundamente que "en Internet la Primera Enmienda es una ordenanza local" [189]. Efectivamente, en cuanto que medio de comunicación, Internet posee unas diferencias radicales con respecto de cualquier otro medio de comunicación, tanto en el plano cuantitativo (su audiencia potencial y la cantidad de información y opiniones accesibles) como en el plano cualitativo (por su nivel de interactividad)[190]. Como afirma Milton Mueller, uno de los retos más críticos de la gobernanza de Internet a nivel mundial es un concepto de libertad de expresión que esté mejor ajustado al sistema de generación de contenidos

[188] BERKMAN CENTER FOR INTERNET AND SOCIETY, *Introduction, Privacy in the Workplace* [en línea]. Disponible en web: https://cyber.harvard.edu/privacy/Module3_Intronew.html#_ftn1

[189] En España Bustamante Donás afirma que "(la libertad de expresión) en el contexto (de la tecnología telemática) no sería sólo uno de los derechos humanos fundamentales, sino también una condición de posibilidad para la defensa y el desarrollo de los demás derechos". BUSTAMANTE DONÁS, J., ob. cit.

[190] DÍAZ REVORIO, F.J., ob. cit., p. 187 y 188.
En referencia a la interactividad, cabe reseñar que el principal exponente de la interactividad es el modelo de Web 2.0 caracterizado precisamente por ese fenómeno. El principal exponente de esta modalidad son las redes sociales y también las denominadas "wikis".

automatizado a gran escala, a los sistemas autónomos interconectados y a capas de acceso altamente diferenciadas, característica del Internet global[191].

No obstante, previo al análisis del régimen jurídico de la libertad de expresión en Internet, es necesario detenernos sucintamente en un presupuesto ontológico de dicha libertad y que constituye el principio sobre el que se cimienta toda la arquitectura de los contenidos en la Red: el principio de neutralidad. Se trata de un principio en el que profundizaremos posteriormente al hilo del tratamiento del derecho a la portabilidad de los datos, en concreto de si es aplicable en entornos de computación en nube; y en caso afirmativo –en línea con el objetivo último de este trabajo –de si para ello resulta adecuado el régimen jurídico actualmente vigente.

A pesar de que se trata de un concepto cuya definición es muy discutida, recurrimos al espíritu descrito en la revista *Scientific American* por Tim Berners-Lee, que recordaba que a principios de los noventa Internet surgió sobre la base de que cualquier persona pudiera compartir información con cualquier otra en cualquier lugar[192]. Y ello, como gráficamente describe David Post, es debido a la forma en la que está organizada la Red. Como señala este autor, uno de los grandes éxitos del desarrollo de Internet es que se ha configurado de tal modo que la capa de red, pudiendo desarrollar muchas más funciones, se limita a la transmisión de mensajes gracias a la configuración *end to end (e2e)*: "máquinas inteligentes conectadas a una red estúpida". Los protocolos TCP/IP no solamente permiten que en cualquier lugar una persona, gracias al enrutamiento distribuido, se conecte a la red, sino que, gracias al diseño e2e, cualquier persona lo haga[193]. Como remata Vinton Cerf, "mediante la instauración de la inteligencia en los bordes más que el control en medio de la red, Internet ha creado una plataforma para la innovación[194]. Tal es su importancia que, como

[191] MUELLER, M.L., *Networks and States. The Global Politics of Internet Governance*, The MIT Press, 2010, 320 p.
[192] BERNERS-LEE, T., Long Live the Web: A Call for Continued Open Standards and Neutrality, *Scientific American,* 22 de noviembre de 2010. Disponible en Web: http://www.scientificamerican.com/article.cfm?id=long-live-the-web
[193] POST, D.G., *In Search of Jefferson´s Moose: Notes on the State of Cyberspace*, Oxford University Press, 2009, 244 p.
[194] Carta dirigida por Vinton Cerf a la Comisión de Energía y Comercio de la Cámara de Representantes de Estados Unidos el 8 de noviembre de 2005. Disponible en Web: https://googleblog.blogspot.com.es/2005/11/vint-cerf-speaks-out-on-net-neutrality.html

afirma dentro de nuestra doctrina García Mexía, “una Internet que no sea neutral, que no sea abierta, podrá seguir siendo una red, pero no será Internet”[195].

Se puede decir que la neutralidad en la red es la I enmienda de la constitución de Internet, aunque no es en absoluto un principio pacífico. Buena prueba del debate existente es la divergencia que existe entre los dos creadores de los Protocolos TCP/IP: por un lado Vint Cerf ha asegurado que "Internet se diseñó sin ningún guardián sobre nuevos contenidos o servicios. Se necesita una regla de neutralidad de red suave pero aplicable para que Internet continúe creciendo."; mientras que Bob Kahn ha calificado de eslogan el término "neutralidad de la red", y ha asegurado que se opone a establecerla, avisando que "nada interesante puede pasar dentro de la red" en el caso de que se apruebe tal neutralidad. "Si el objetivo es animar a la gente a construir nuevas capacidades, entonces alguien tiene que dirigir el camino para construir esa nueva capacidad, y probablemente sólo lo va a hacer en su red, no en la red de otros"[196]. En el plano oficial, un claro ejemplo de la existencia de debate fue la Orden aprobada por la Comisión Federal de Comunicaciones el 21 de diciembre de 2010 para preservar un Internet abierto[197] que fue aprobada por una ajustada votación y que se asienta sobre los principios de transparencia, no bloqueo y discriminación no justificada[198]. Más recientemente, el 26 de febrero de 2015[199], de nuevo la referida Comisión aprobó una serie de normas sobre neutralidad en la red (consideradas por Tim Wu como las más estrictas nunca aprobadas)[200] de nuevo por un ajustado resultado de 3 a 2. Fue precisamente este autor el que teorizó el contenido del principio de neutralidad resumiéndolo con una acertada y gráfica frase: “el interés en promocionar la neutralidad en la red es preservar una competitividad darwiniana entre cualquier uso concebible de Internet de tal modo que solamente el mejor sobreviva”[201].

---

[195] GARCÍA MEXÍA, P.L., *Historias de Internet. Casos y cosas de la red de redes*, Valencia: Tirant Humanidades, 2012, 167 p.

[196] http://es.wikipedia.org/wiki/Neutralidad_de_red

[197] Sirva como curiosidad que Internet abierto es la expresión preferida por la compañía Google frente al concepto de neutralidad en la red y así lo manifestó en el debate sobre esta cuestión organizado por Elmundo.es el 11 de noviembre de 2010 http://www.elmundo.es/elmundo/2010/11/19/navegante/1290182664.html

[198] El texto completo del Informe y la Orden derivada del mismo (FCC 10-201) se encuentra en http://www.fcc.gov/Daily_Releases/Daily_Business/2010/db1223/FCC-10-201A1.pdf

[199] Esta normativa adoptada por la FCC tienen una particular trascendencia y básicamente suponía

[200] WU, T., Why everyone was wrong about Net Neutrality?, *New York Times*, 26 de febrero de 2015. Disponible en web: http://www.newyorker.com/business/currency/why-everyone-was-wrong-about-net-neutrality

[201] WU, T., Network Neutrality, Broadband Discrimination, *Journal on telecom and high tech law*, 2003, vol. 2, p. 141-179.

Desde el punto de vista normativo, las sociedades más avanzadas han recogido esta norma, no sin polémica. Así, en Estados Unidos, la FCC, en su mencionada decisión de 26 de febrero de 2015 establecía básicamente mediante la reclasificación del acceso de banda ancha como un servicio de telecomunicaciones y consiguientemente aplicándoles el Título II de la Ley de Comunicaciones de 1934, que hace referencia a los servicios generales (*common carrier*). En el caso de la Unión Europea, también se dio un paso relevante a través del Reglamento (UE) 2015/2120 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 por el que se establecen medidas en relación con el acceso a una internet abierta y se modifica 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 y el Reglamento (UE) no 531/2012 relativo a la itinerancia en las redes públicas de comunicaciones móviles en la Unión (Texto pertinente a efectos del EEE). Como reza el primero de sus considerandos, su finalidad es establecer normas comunes destinadas a garantizar un trato equitativo y no discriminatorio del tráfico en la prestación de servicios de acceso a internet y a salvaguardar los derechos de los usuarios finales.

3.2.2.2 Libertad de expresión en Internet: censura y el derecho de acceso a la red.

Una vez realizado este repaso al principio de neutralidad en la red y apuntado el debate existente, vamos a analizar la libertad de expresión desde una doble perspectiva: por un lado como instrumento esencial de una sociedad democrática y los retos a los que se enfrenta en el marco de las sociedades no democráticas, puesto que "el ciberespacio aparece como uno de los escenarios donde se dirime una de las más decisivas batallas por la libertad de expresión"[202]; y por otro, los límites que existen a la libertad de expresión e información y en qué medida cabe aplicar los instrumentos tradicionales en Internet a efectos de dicha limitación. Todo ello acompañado de apuntes referidos al derecho de acceso y a la protección de la infancia o los discursos de odio. Terminaremos con un detallado tratamiento de uno de los elementos clave de la libertad de expresión: el régimen de responsabilidad de los prestadores de servicios de intermediación.

Respecto a la primera cuestión, una gran prueba de la importancia del impacto de la Red de redes en la libertad de expresión es el mapa de censura de Internet.

[202] BUSTAMANTE DONÁS, J., ob. cit.

Fuente: *Reporteros sin Fronteras*

Como afirma el profesor Rubio Moraga, existen muy diferentes formas de ejercer la censura en Internet en función de las características del país en el que nos encontremos[203]: la prohibición del acceso a Internet, caso de Corea del Norte; permitir el acceso a la Red sobre la base de un restrictivo control basado en autorizaciones a personas "de confianza", caso de Cuba; la monitorización como en el caso China, Rusia, Singapur, India o algunos países de África del Norte y de Oriente Medio; el filtro de contenidos y bloqueo de determinadas Web, como en el caso de Arabia Saudí; algunas otras medidas más propias de países avanzados democráticamente que, sin ser supuestos de censura, bajo el pretexto de la protección de otros bienes jurídicos establecen leyes, propuestas de regulación o el uso de redes espía como *Echelon* o programas como *Carnivore*.

[203] RUBIO MORAGA, A.L., Censura en la Red: restricciones a la libertad de expresión en Internet; en SANZ ESTABLÉS, C., SOTELO GONZÁLEZ, C. RUBIO MORAGA, A.L (Coords.), *Prensa y periodismo especializado II*, 2004, p. 597-607.

Frente a estas realidades, Internet se ha demostrado sin embargo como un instrumento básico en el ejercicio de la libertad de expresión, haciendo frente precisamente a estos controles. Ejemplos tenemos a lo largo de los últimos años: caso de Tiananmen durante cuyos acontecimientos en 1990 Internet sirvió para que la comunidad china conociera, especialmente en las universidades, la realidad de lo que estaba ocurriendo; el golpe de Estado en Rusia (1991) cuando una red de ordenadores rusa llamada Relcom mantuvo informados a los ciudadanos rusos frente al apagón informativo; durante la invasión de Kuwait en 1991 se hizo famoso el *Internet Relay Chat*, que consiguió mantenerse operativo incluso cuando las señales de radio y televisión habían sido cortadas.; en Yugoslavia en 1996, una emisora de Radio ejerció su derecho a la libertad de expresión y mantuvo su señal a través de Internet cuando los medios tradicionales ya no podían; de manera similar a como sucedió en Honduras cuando Radio Globo fue sacada del aire (pero no de línea) durante el último golpe de estado. También podemos pensar en las revoluciones que a finales del 2010 y comienzos de 2011 afectaron al mundo árabe y en las que Internet si no una causa principal, sí jugó un papel principal. No en vano, uno de los mayores expertos en el impacto de la red en la distribución del poder, el profesor Manuel Castells, las bautizó como "la wikirevolución del jazmín"[204].

Y es que Internet ha alterado sustancialmente la libertad de expresión. De nuevo, al igual que hemos visto en el caso del derecho a la intimidad, no estamos hablando de un derecho que se haya visto alteado cuantitativamente, por una mayor capacidad de llegada, sino que la alteración ha sido cualitativa. Así se ha venido en reconocer en documentos oficiales como la Declaración Conjunta sobre Libertad de Expresión e Internet del Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión, la Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Relatora Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión y la Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP) en 2011, donde se destacaba el carácter transformador de Internet, como medio que permite que miles de millones de personas en todo el mundo expresen sus opiniones, a la vez que incrementa significativamente su capacidad de acceder a información

[204] CASTELLS, M., La Wikirevolución del jazmín, *La Vanguardia*, 29 de enero de 2011. Disponible en Web: http://www.lavanguardia.es/opinion/articulos/20110129/54107291983/la-wikirrevolucion-del-jazmin.html

y fomenta el pluralismo y la divulgación de información[205]. Y también se recoge en diferentes posicionamientos doctrinales, como cuando Fernández Esteban subrayaba "La importancia de Internet para la libertad de expresión no se debe sólo a que es un acontecimiento planetario, cuyas tasas de crecimiento desbordan todas las previsiones, sino en que por vez primera cualquier usuario de Internet puede airear sus puntos de vista, haciéndolos llegar a millones de otras personas, a través de los grupos de discusión o de la publicación de datos, información o imágenes en su página de Internet"[206]. El referido La Rue subrayaba con claridad este cambio de naturaleza que Internet ha dado a la libertad de expresión, con base en un triple argumento: porque Internet permite una comunicación bidireccional, haciendo del usuario final no solamente un receptor pasivo de información sino un editor activo; porque hace posible una distribución asequible de cualquier tipo de contenido, dando así acceso a información y conocimiento que previamente era inaccesible; y porque permite la comunicación en tiempo real[207]. A dichos argumentos añade Balkin otra perspectiva y es que permite que la libertad de expresión actúe como un catalizador que enfatiza no solamente una sociedad democrática sino una cultura democrática[208].

Observamos por tanto que la naturaleza esencial de la libertad de expresión en Internet se ve sin embargo precedida por otro derecho que ya ha sido mencionado más arriba en pronunciamiento de Naciones Unidas: el derecho de acceso a Internet. Estamos de nuevo ante un presupuesto ontológico para hacer realidad el derecho a la libertad de expresión en Internet. En palabras de Manuel Castells, "la única censura posible de Internet es no estar en la red"[209].

Cuestión distinta es si estamos únicamente ante un presupuesto frente a otros derechos o si estamos ante un derecho fundamental en sí mismo[210]. Aquí hay autores como Brownsword

---

[205] ORGANIZACIÓN DE ESTADOS AMERICANOS. Declaración Conjunta sobre Libertad de Expresión e Internet, 2011. Disponible en web: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849

[206] FERNÁNDEZ ESTEBAN, M.L., La libertad de expresión en Internet, *Nueva Revista*, agosto 1999, nº 64. Disponible en Web: http://www.nuevarevista.net/articulos/la-libertad-de-expresion-en-internet

[207] LA RUE, F., *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. United Nations, 2011. Disponible en web: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

[208] BALKIN, J.M., Digital speech and democratic culture. *New York University Law Review*, 2004, vol. 79, nº 1, p. 1-55.
Disponible en web: http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1239&context=fss_papers

[209] CASTELLS, M., Internet, libertad y sociedad: una perspectiva analítica, *Polis, Revista de la Universidad Bolivariana,* 2003, vol. 1, núm. 4.

[210] Una exposición de los argumentos a favor y en contra del reconocimiento del derecho de acceso a Internet como un derecho fundamental en DE HERT, P. y KLOZA, P., Internet (access) as a new fundamental right. Inflating the current rights framework?', *European Journal of Law and Technology*, 2012, Vol.3, nº 3.

y Goodwin que sostienen que hay nuevos derechos en el horizonte, en línea con lo que hemos defendido al principio de este capítulo, que incluirían derechos como el de la intimidad genética, el derecho a una identidad único o el derecho de acceso a Internet[211]; mientras que sin embargo voces como la de Vinton Cerf rechazan dicha consideración afirmando que Internet es valioso en cuanto que medio para un fin, pero no en cuanto que un fin en sí mismo[212].

También se han dado pronunciamientos de naturaleza política respecto a esta cuestión. Uno de los pioneros por cierto fue el Senado español que, en las Conclusiones de la Comisión Especial de Redes Informáticas, aprobadas por el Pleno de la Cámara el 17 de diciembre de 1999, señalaba[213]: "Todas las personas tienen el derecho fundamental de acceder libremente a la Red, sin discriminación de sexo, condición, características físico-psíquicas, edad o lugar de residencia". La *Internet Rights and Principles Dynamic Coalition*, en su Carta de Derechos Humanos y Principios en Internet recoge que "Toda persona tiene derecho a acceder a Internet. En este derecho se basan todos los demás derechos en esta Carta"[214]. El Centro Nexa par Internet y la Sociedad, de la Universidad Politécnica de Turín, en el artículo 2.1 de su propuesta de dice: "El acceso a Internet es un derecho fundamental de la persona y una condición para su pleno desarrollo individual y social"[215]. En un ámbito más oficial, la Asamblea del Consejo de Europa, en su Resolución 1987 de 2014 recomendaba que los Estados miembros aseguren el derecho de acceso a Internet[216]. En el caso de Naciones Unidas, y además del pronunciamiento ya citado de 2011, más recientemente, en julio de 2016 el Consejo de Derechos Humanos aprobó una Resolución en la que consideraba la interrupción del acceso a Internet como una vulneración de los derechos humanos[217]. Por su

[211] DE HERT, P. y KLOZA, P., ob. cit. Disponible en web: http://ejlt.org/article/view/123/268#_ednref31
[212] CERF. V., Internet Access Is Not a Human Right, *New York Times*, 4 de enero de 2012.Disponible en web: http://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html .
[213] SENADO. Comisión Especial de Redes Informáticas. Informe Final. Boletín Oficial de las Cortes Generales, Senado, Serie I, nº 812, 27 de diciembre de 1999.
[214] INTERNET RIGHTS AND PRINCIPLES DYNAMIC COALITION. Carta de Derechos Humanos y Principios en Internet. Disponible en Web: http://diadeinternet.org/pdfs/Internet_Derechos_Principios.pdf
[215] NEXA CENTER FOR INTERNET&SOCIETY. Declaración de los derechos en Internet. Disponible en web: https://nexa.polito.it/nexacenterfiles/dichiarazione-diritti-internet-spagnolo.pdf
[216] COUNCIL OF EUROPE. Assembly. Resolution 1987 (2014). 9 de abril de 2014. Disponible en Web: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=20870&lang=en
[217] UNITED NATIONS. Human Rights Council. The promotion, protection and enjoyment of human rights on the Internet. 12 de julio de 2016. Disponible en Web: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

parte, la Unión Europea habla del derecho de acceso a Internet en su Código de derechos en línea, publicado por la Comisión Europea en diciembre de 2012[218].

Sin embargo, no estamos hablando de un debate meramente doctrinal o de una pura declaración de intenciones voluntarista, sino que existen incluso reconocimientos desde el punto de vista normativo. Son varios los textos, de uno u otro rango, que han ido recogiendo este derecho. A nivel constitucional, fue en el año 2001 cuando Grecia modificó su Constitución para introducir, entre oros cambios, que "toda persona tiene derecho a participar en la Sociedad de la Información". Y el párrafo añade que "facilitar el acceso a la información transmitida electrónicamente, el intercambio y difusión consiguientes, constituye una obligación del Estado". En el caso de Estonia, fue ya en el año 2000, cuando se aprobó la Ley de Telecomunicaciones, incluyendo el acceso a Internet dentro del listado de servicios universales. También en Finlandia que introdujo una modificación a la Ley de Mercado de las Comunicaciones recogiendo igualmente que el concepto de servicio universal incluye una conexión funcional a Internet. Y en esta línea del servicio universal, se incluiría a España en 2011 y es hoy el artículo 25.1.a) el que señala: "Todos los usuarios finales puedan obtener una conexión a la red pública de comunicaciones electrónicas desde una ubicación fija siempre que sus solicitudes se consideren razonables en los términos que mediante real decreto se determinen y que, incluirán, entre otros factores, el coste de su provisión. La conexión debe permitir realizar comunicaciones de voz, fax y datos, a velocidad suficiente para acceder de forma funcional a Internet. La conexión a la red pública de comunicaciones con capacidad de acceso funcional a Internet deberá permitir comunicaciones de datos en banda ancha a una velocidad en sentido descendente de 1 Mbit por segundo". En fin, en la reforma operada en 2013, la Constitución de los Estados Unidos Mexicanos, en su artículo 6 recogía que "El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios".

[218] EUROPEAN COMMISSION. Code of EU online rights. Diciembre de 2012. Disponible en web: https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/Code%20EU%20online%20rights%20EN%20final%202.pdf

En otras ocasiones ha sido la jurisprudencia la que ha reconocido este derecho. En Francia fue el Consejo Constitucional quien, en su Sentencia de 10 de junio de 2009[219], al pronunciarse sobre la conocida Ley Hadopi, señaló que en el estado actual de los medios de comunicación y con respecto al desarrollo generalizado de los servicios de comunicación pública en línea así como a la importancia que tienen estos servicios para la participación en la vida democrática y la expresión de ideas y opiniones, la libre comunicación de pensamientos y opiniones implica la libertad de acceder a estos servicios. Por su parte, en Costa Rica, en una conocida Sentencia de 30 de julio de 2010[220], se afirmó de manera expresa la existencia de un derecho constitucional de acceso a las nuevas tecnologías y un derecho de acceso a Internet a través de una interfaz que el usuario y el consumidor elige.

Podemos concluir por tanto que el derecho de acceso a Internet constituye un presupuesto, en su vertiente jurídica y lógicamente en la tecnológica, para poder hacer realidad el derecho a la libertad de expresión en sí misma. En cuanto a su consideración como derecho fundamental *per se* y pensando en la trascendencia que esta categoría puede tener en el plano práctico, su inclusión en el contenido propio del derecho a la libertad de expresión en Internet facilita hoy día su universalización, por cuanto aquel es un derecho genéricamente conocido, sin perjuicio de que exista una tendencia en sí misma -aún en fase de larva como dice Cotino Hueso[221]- que lleva a su consideración como un derecho fundamental autónomo. Pensando en el objetivo último de este trabajo, en la utilidad del marco normativo actual para el fenómeno de la computación en nube, el derecho de acceso lo es todo. Si algo caracteriza a la computación en nube es la ubicuidad, la capacidad de acceso en cualquier momento y lugar a la información. El acceso a la red es equivalente en la nube al acceso a nuestro ordenador en nuestro domicilio o en nuestro lugar de trabajo, y por tanto adquiere una mayor relevancia si cabe.

Resta por tratar, como hemos apuntado, los límites que existen a la libertad de expresión e información y en qué medida cabe aplicar los instrumentos tradicionales en Internet a efectos de dicha limitación. Debemos subrayar que, a diferencia de lo acontecido con la intimidad

[219] Francia. Consejo Constitucional. N°2009-580. Sentencia de 10 de junio de 2009. Acceso al texto de la Sentencia en el siguiente enlace: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009580DCes2009_580dc.pdf
[220] Costa Rica. Sala Constitucional. Sentencia nº 10627 de 30 de julio de 2009.
[221] COTINO HUESO, L., Las obligaciones del Estado: el nuevo derecho fundamental de acceso a internet y las garantías a partir de la redefinición de las clásicas libertades informativas, en AA.VV, *La responsabilidad del Estado por la utilización de las tecnologías de la información y la comunicación (TIC)*, Universidad Católica de Colombia, Bogotá, 2015, p. 51-94.

que es un derecho que como hemos visto se ha visto seriamente amenazado como consecuencia de determinados usos de Internet, en el caso de la libertad de expresión, el debate radica en la necesidad de establecer límites y quiénes son los responsables por los contenidos vertidos en Internet. Todo ello sin perjuicio de los grandes problemas que se plantean como los derivados de los diferentes estándares de protección de la libertad de expresión en Estados Unidos y en Europa que ya hemos visto en su vertiente clásica. Sirva como un ejemplo de estos estándares el de uno de los casos más conocidos y de mayores implicaciones en la historia de la regulación jurídica de Internet, ya que planteó un debate sobre la propia esencia de Internet: el caso *Yahoo*. Se trataba de la posibilidad de subasta y venta de objetos nazis en la Web de Yahoo. El caso muestra muy claramente, además de otros problemas, los diferentes estándares de protección y límites a la libertad de expresión y en qué medida en Internet se multiplica este problema debido a su accesibilidad universal. Los tres estadios de este caso fueron[222]:

- La decisión del Tribunal de Gran Instancia de París en la demanda interpuesta a por dos grupos judíos (LICRA y UEJF) con la intención de cerrar o bloquear el acceso de los usuarios franceses a dicha Web, situada en los Estados Unidos. El Tribunal ordenó el bloqueo del acceso de los usuarios franceses a dicha Web.
- La decisión del Tribunal Federal del Distrito Norte de California en noviembre de 2001, tras la acción judicial de *Yahoo*, que afirmaba que estábamos ante una manifestación de la libertad de expresión protegida por la Primera Enmienda y que *Yahoo* no está en modo alguno obligada a acatar la legislación francesa en materia de contenidos en Internet en webs radicadas en Estados Unidos.
- La tercera fase trae causa de la Sentencia de febrero de 2002 en la que el Tribunal Correccional de París, como consecuencia de la denuncia interpuesta por ADA (otro grupo judío) en la que se reclamaba la plena competencia de los tribunales franceses y la plena aplicabilidad de la legislación francesa por tratarse de una Web accesible desde Francia.

Este planteamiento de diferentes estándares no solamente ha tenido reflejo jurisprudencial, sino que también ha sido objeto de posicionamientos doctrinales. Como señala Pollicino, en Estados Unidos la llegada de Internet no ha supuesto una merma en la protección otorgada por los tribunales a la libertad de expresión. Al revés, parece que la efectividad de la libertad

[222] Tomado de GARCÍA MEXÍA, P., *Derecho Europeo de Internet,* ob. cit., p. 105 y ss.

de expresión se ha visto mejorada, en particular a través de un escrutinio muy estricto de las condiciones que pueden suponer una base jurídica para restringir esta libertad. Sin embargo, señala el autor, en este caso tras atender a la STEDH de 18 de diciembre de 2012 (caso *Ahmet Yildirim vs Turkey*)[223], considera que este tribunal, vistos los riesgos que trae consigo internet, está más por limitar la libertad de expresión en Internet que en un contexto no digital.[224]

Al margen de estos estándares, en ambos casos, como es propio de las sociedades avanzadas, el debate radica en cuanto a los límites del derecho a la libertad de expresión. El Tribunal Supremo de los Estados Unidos tuvo la oportunidad de pronunciarse sobre la materia en la Sentencia de 1997 en el caso *ACLU* vs. Reno[225], caso especialmente relevante porque fue la primera vez que atendió específicamente a los contenidos en Internet y anuló determinadas previsiones de la *Communications Decency Act* por ser contrarias a la Primera Enmienda. Con la finalidad de proteger a los menores de materiales apropiados en Internet, la ley criminalizaba la transmisión intencionada de mensajes "obscenos o impúdicos", así como la transmisión de información que describa o muestre "actividades sexuales u órganos excretores" de una forma "ofensiva" para los estándares comunitarios. El Tribunal Supremo consideró que las definiciones de los tipos de comunicaciones en Internet que penalizaba eran demasiado vagas y consiguientemente vulneraban la Primera Enmienda. La clave de la decisión, como explica la profesora Fernández Esteban[226], fue la equiparación de la navegación por Internet con la prensa escrita y no con la radiodifusión, que tiene unos límites mayores a la libertad de expresión que la prensa escrita[227]. Asimismo el Tribunal afirmaba que existen métodos para limitar la libertad de expresión como los programas-filtro, menos nocivos que la prohibición; y por último recordaba que Internet puede salvar la teoría del "mercado de las ideas" debido a sus efectos democratizadores y a la diversidad que introduce en ese mercado de las ideas. También en la misma línea argumental, es relevante en el caso

[223] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Sección segunda). Caso Ahmet Yildirim vs Turquía. Sentencia de 18 de diciembre de 2012.
[224] POLLICINO, O., European Judicial Dialogue and the Protection of Fundamental Rights in the New Digital Environment: An Attempt at Emancipation and Reconciliation, en MORANO-FOADI, S. y VICKERS L. (eds.), *Fundamental Rights in the EU: A Matter for Two Courts*, Blomsbury, 2015, p. 93-114.
[225] Estados Unidos. Tribunal Supremo. Caso ACLU vs. Reno. Sentencia de 26 de junio de 1997. Acceso al texto de la sentencia en el siguiente enlace: https://www.aclu.org/legal-document/supreme-court-decision-reno-v-aclu-et-al
[226] FERNÁNDEZ ESTEBAN, M.L., La regulación de la libertad de expresión en Internet en Estados Unidos y en la Unión Europea, *Revista de estudios políticos*, 1999, nº 103, p. 162 y ss.
[227] Los motivos en los que justificaba esta equiparación fueron principalmente que las comunicaciones a través de Internet no "invaden" la casa del individuo o aparecen en la pantalla del usuario si éste no las busca en la Red. *Idem*, p. 163.

de Estados Unidos, la Sentencia de 16 de abril de 2002[228] del Tribunal de Apelación del Noveno Circuito en el caso *Ashcroft v. Free Speech Coalition* en el que se declaró inconstitucional la Ley de Prevención de la Pornografía Infantil de 1996 por considerar que sus previsiones iban más allá de lo admisible, ya que las restricciones eran excesivas y vulneraban la primera enmienda.

3.2.2.3 Algunos límites a la libertad de expresión: juventud, infancia y discursos de odio.

En este campo, uno de los sectores que más ha preocupado, y del que ya hemos reflejado algún ejemplo, es el de la juventud y la infancia. Se trata de una cuestión sobre la que los Estados sí han entrado a regular, máxime cuando nos encontramos con que la juventud y la infancia constituyen una parte esencial de los usuarios de Internet.

En Estados Unidos esta cuestión se afrontó a través de la ya citada Ley de Decencia en las Telecomunicaciones que se basaba en la necesidad de proteger a los menores de material indeseable o dañino presente en Internet que llegaba a prohibir el material "indecente" amparado por la Primera Enmienda y cuya publicación se consideraba legal en la prensa escrita. Como consecuencia de la Sentencia *ACLU vs. Reno* antes mencionado, se dictaron otras dos normas: la Ley para un Internet Seguro en las Escuelas (*Safe Schools Internet Act*)[229] y la Ley de Protección Infancia en línea (*Child Online Protection Act)*[230], norma que fue considerada de nuevo inconstitucional, tras un largo proceso judicial que culminó con la Sentencia de 22 de julio de 2008 del Tribunal de Apelaciones del Tercer Circuito de los Estados Unidos[231] y cuya apelación no fue admitida a trámite por el Tribunal Supremo en su decisión de 21 de enero de 2009.

Otro intento fue la Ley de Protección de la Infancia en Internet (*Children's Internet Protection Act*) para controlar el material que pueda ser nocivo para los menores en Internet, si bien es cierto que su ámbito de actuación era más reducido que las dos anteriores. Lo que pretende

---

[228] Estados Unidos. Corte de Apelación del Noveno Circuito. Caso Ashcroft vs. Free Speech Coalition. Sentencia de 16 de abril de 2002. Acceso al texto de la Sentencia en el siguiente enlace: https://www.supremecourt.gov/Search.aspx?FileName=/docketfiles/00-795.htm

[229] Esta ley requiere que toda escuela, instituto o biblioteca que reciba fondos públicos deba instalar programas filtro.

[230] Conocida también como *Congress Decency Act II*.

[231] Estados Unidos. Tribunal de Apelaciones del Tercer Circuito. Caso ACLU vs. Mukhasey. Sentencia de 22 de julio de 2008. Acceso al texto de la Sentencia en el siguiente enlace: http://www2.ca3.uscourts.gov/opinarch/072539p.pdf

esta norma es que las bibliotecas públicas que reciben fondos públicos instalen software de filtrado en cualquier ordenador con acceso a Internet para bloquear imágenes obscenas o de pornografía infantil y también busca prevenir a los menores del acceso a material que les pueda resultar dañino. CIPA fue igualmente llevada ante el Tribunal Supremo en el caso *US vs. Library Association*[232] y en su decisión la CIPA fue confirmada, si bien es cierto que el impacto de la ley es limitado, puesto que solamente se aplica, subrayamos, en el acceso a Internet a través de los dispositivos de las bibliotecas.

En fin, hay otras disposiciones como la 18 USC § 2425, que prohíbe el uso de Internet para transmitir información sobre un menos de 16 años para fines sexuales. Las personas condenadas en virtud de esta ley se enfrentan a una pena de multa y/o a una pena de prisión de hasta cinco años. Y los legisladores americanos han añadido también el uso de ordenadores e Internet a las actuales prohibiciones penales destinadas a proteger la seguridad física de los niños. Por ejemplo, atraer a los niños es una conducta prohibida en virtud de 18 USC § 2422 b), incluyendo la utilización de cualquier dispositivo de Internet para persuadir conscientemente, inducir, seducir o coaccionar a un menor para participar en una actividad delictiva de naturaleza sexual o para prostituirse. La pena que se contempla es de multa y una pena de prisión que como mínimo es de diez años y que puede llegar a la cadena perpetua.

En Europa, desde muy temprano se puso ya de manifiesto la necesidad de proteger al menor, pero sin dejar de hacer mención a su equilibrio con la libertad de expresión. Así, en la Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones sobre los contenidos ilícitos y nocivos en Internet, así como en el Libro Verde sobre la protección de los menores y de la dignidad humana en los servicios audiovisuales y de la información de 1996 "…es imprescindible que las iniciativas internacionales tengan en cuentan las distintas normas éticas de los diversos países con el fin de sondear las normas adecuadas para la protección de la población frente a los materiales ofensivos, garantizando al mismo tiempo la libertad de expresión". Con posterioridad se han ido desarrollando en diversos instrumentos. El primero de ellos digno de mención fue el Plan de Acción para una

[232] Estados Unidos. Tribunal Supremo. Caso US vs. American Library Association. Sentencia de 23 de junio de 2003. Acceso al texto de la sentencia en el siguiente enlace: https://www.law.cornell.edu/supct/html/02-361.ZO.html

utilización de Internet más segura[233]. Las acciones que contemplaba eran muy variadas, incluyendo algunas relacionadas con la libertad de expresión como la de ofrecer a la población y fomentar la existencia de puntos de contacto y teléfonos de información y asistencia permanente que faciliten la denuncia de los contenidos ilícitos y las conductas nocivas en línea; o fomentar la aplicación de soluciones técnicas para hacer frente adecuadamente al uso por parte de los usuarios finales de filtros que impidan el paso a través de las tecnologías en línea de información que pueda vulnerar la integridad física, mental o moral de los niños; o alentar y ayudar a los proveedores de servicios de Internet a desarrollar, como instrumento de autorregulación, una etiqueta "seguro para los niños" para las páginas web.

Otros instrumentos jurídicos de que dispone la Unión Europea son la Decisión del Consejo 2000/375/JAI de 29 de mayo de 2000 relativa a la lucha contra la pornografía infantil en Internet y la Decisión marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil. La primera contempla, entre otras, la necesidad de alentar a los usuarios de Internet a indicar a las autoridades represivas los casos de presunta difusión de material pornográfico infantil en Internet. Por su parte, la Decisión de 2004 contempla una serie de comportamientos punibles que constituyen una "infracción relacionada con la pornografía infantil" se realicen mediante sistemas informáticos o no. Más recientemente, las Directrices de la UE sobre derechos humanos relativas a la libertad de expresión en Internet y fuera de Internet de 12 de mayo de 2014 recogía que se recurrirá a todas las directrices vigentes de la UE en materia de derechos humanos, cuando sean aplicables, al tratar las posibles violaciones del derecho a la libertad de opinión y de expresión, en particular las directrices para la promoción y protección de los derechos del menor.

[233] El programa se articuló a través de la Decisión nº 276/1999/CE del Parlamento Europeo y del Consejo, de 25 de enero de 1999, por la que se aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales. Este programa, que sufrió alguna modificación normativa y que duraba hasta el 31 de diciembre de 2004, se prorrogó mediante la Decisión n° 854/2005/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, por la que se crea un programa comunitario plurianual para el fomento de un uso más seguro de Internet y las nuevas tecnologías en línea, conocido como *Safer Plus*. Posteriormente estuvo vigente el Programa *Safer Internet* implementado para el periodo 2009-2013 a través de la Decisión 1351/2008/CE del Parlamento Europeo y del Consejo, de 16 de diciembre de 2008, por la que se establece un programa comunitario plurianual sobre la protección de la infancia en el uso de Internet y de otras tecnologías de la comunicación

En el ámbito Consejo de Europa, además de otras, hay que destacar el Convenio sobre Cibercriminalidad que recoge los siguientes comportamientos punibles: la producción de pornografía infantil con la intención de difundirla a través de un sistema informático; el ofrecimiento o la puesta a disposición de pornografía infantil a través de un sistema informático; la difusión o la transmisión de pornografía infantil a través de un sistema informático; el hecho de procurarse o de procurar a otro pornografía infantil a través de un sistema informático y la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos. En la misma línea se ha de recordar la Convención del Consejo de Europa para la protección de la infancia contra la explotación sexual y el abuso sexual. En lo que nos afecta el convenio contempla dos tipos de medidas: preventivas, destinadas a la educación de los niños especialmente en el uso de las TIC (art. 6) y la participación del sector empresarial tecnológico en estas políticas de prevención a través incluso de mecanismos de autorregulación (art. 9); y sustantivas, con la introducción de determinados tipos delictivos (arts. 18 a 23).

Además de la juventud y de la infancia, existen otros límites, entre los cuales destaca el honor de las personas o los límites a la incitación al odio. De nuevo se debe subrayar que no estamos ante algo novedoso, estos conflictos ya existían antes de Internet. La diferencia radica en la "viralidad", en términos modernos, que puede causar la ofensa o el discurso de odio y las consecuencias que pueden tener para las sociedades democráticas. La normativa y la doctrina se han pronunciado sobre estas cuestiones. Como todo derecho fundamental, sus límites han de estar muy tasados. Recordemos en el plano normativo el artículo 10.2 CEDH, el artículo 17 del mismo texto que prohíbe el abuso de derechos, o el artículo 52 CDFUE. O en un escalón inferior, la Decisión marco 2008/913/JAI del Consejo relativa a la lucha contra determinadas formas y manifestaciones de racismo y xenofobia mediante el Derecho penal. E incluso inevitables y necesarios ejemplos de colaboración público privada, caso, en gran medida como consecuencia de la propaganda terrorista en las redes, del Código de Conducta[234] elaborado por la Comisión Europea y un grupo de empresas tecnológicas (Facebook, Twitter, YouTube y Microsoft) que incluye una serie de compromisos para luchar contra la propagación de la incitación ilegal al odio en Internet en Europa.

[234] EUROPEAN COMMISSION. Code of conduct on countering ilegal hate speech online. 2016. Acceso al Código de Conducta en versión inglesa en el siguiente enlace: http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf

Pero, como resulta lógico, ha sido fundamentalmente la jurisprudencia la que ha tenido que lidiar con este fenómeno de hasta dónde puede llegar la libertad de expresión, siendo de nuevo el TEDH una referencia en la materia por haber venido marcando una serie de principios a tener en cuenta[235]: tras recordar, como hemos visto más arriba, que el artículo 10 CEDH resulta aplicable a Internet en cuanto que medio de comunicación por lo que nos limitaremos a señalar los puntos más importantes. Así, señala por ejemplo que la libertad de expresión en el plano político tiene un grado de protección superior, así en la STEDH de 23 de abril de 2015 (caso *Morice vs. France*)[236]. Particularmente relevante resulta en este sentido la STEDH de 5 de mayo de 2011 (caso *Editorial Board of Pravoye Delo and Shtekel vs. Ukraine*)[237] donde el Tribunal señaló por primera vez, precisamente en conexión con ese grado de libertad en cuanto a la opinión política y sobre cuestiones de interés general, que el artículo 10 tiene que ser interpretado en cuanto que impone a los Estados una obligación de crear un marco normativo adecuado para asegurar la protección efectiva de la libertad de expresión de los periodistas en Internet. En este campo de los límites, también merece la pena hacer una mención el tratamiento que se hace de la sátira, la STEDH de 18 de octubre de 2005 (caso *Perrin vs. UK)*[238] afirmaba que la libertad de expresión ampara informaciones que ofenden, chocan o molestan al Estado o a un sector de la población y añade que así lo exige el pluralismo, la tolerancia y la apertura de mente sin las cuales no hay una sociedad democrática; pero igualmente inadmite el recurso cuando deriva en comentarios injuriosos u ofensivos[239]. Por último, cabe señalar, como no podía ser de otro modo, que la adecuada técnica de la ponderación es la que se utiliza en los conflictos entre la libertad de expresión y el derecho a la intimidad, consustancial al devenir de ambos a lo largo de la historia. En este sentido, como resume la propia División de Documentación del TEDH, este se limita a verificar que se han ponderado los criterios adecuados por parte del tribunal nacional[240]: la

[235] La mayoría de las referencia jurisprudenciales extraídas del magnífico compendio del propio TEDH. COUNCIL OF EUROPE. *Internet: case-law of the European Court of Human Rights*, 2015. Disponible en web: http://www.echr.coe.int/documents/research_report_internet_eng.pdf

[236] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Gran Sala). Caso Mourice vs. France. Sentencia de 23 de abril de 2015. Acceso al texto de la Sentencia en el siguiente enlace: http://www.echr.coe.int/documents/research_report_internet_eng.pdf

[237] Consejo de Europa. Tribunal Europeo de Derechos Humanos (sección quinta). Caso Editorial Board of Pravoye Delo and Shtekel vs. Ukraine. Sentencia de 5 de mayo de 2011. Acceso al texto de la Sentencia en el siguiente enlace:

[238] Consejo de Europa. Tribunal Europeo de Derechos Humanos (sección cuarta). Caso Perrin vs. UK. Sentencia de 18 de octubre de 2005. Acceso al texto de la Sentencia en el siguiente enlace: http://echr.ketse.com/doc/5446.03-en-20051018/view/

[239] Consejo de Europa. Tribunal Europeo de Derechos Humanos (sección cuarta). Caso Bartnik v. Poland. Decisión de 11 de marzo de 2014. Acceso al texto de la Decisión en el siguiente enlace: https://cases.legal/en/act-echr1-142318.html

[240] COUNCIL OF EUROPE. *Internet: case-law of the European Court of Human Rights*, ob. cit., p. 21.

contribución a un debate de interés general, si la persona es pública o no, el objeto de la información, la forma y la repercusión de la publicación y la proporcionalidad o severidad de la pena impuesta.

En fin, al margen de centrar el debate en Estados Unidos y Europa, por su particular paralelismo a la par que diferente aproximación, no podemos dejar de tener en cuenta otras latitudes. Por ejemplo, en el campo del derecho al honor y también a la propia imagen, ha sido de especial atención el mundo de las redes sociales. Así, en Colombia su Corte Constitucional, en Sentencia de 10 de febrero de 2016,[241] recordaba que "lo "publicado en redes sociales está amparado por la libertad de expresión, pero también está sujeto a los límites…, implicando que las manifestaciones difamatorias, groseras e insultantes, entre otras, no se encuentran bajo la protección señalada en el artículo 20 de la Carta, ni por los instrumentos internacionales que la consagran". O en otro continente, la muy relevante Sentencia de 24 de marzo de 2015 (caso *Shreya Singhal vs. Union of India*)[242] del Tribunal Supremo de la India, en la que anulaba el artículo 66A de la Ley de Tecnología de la Información de 2000 por considerar que sus previsiones tenían un efecto paralizador en el derecho a la libertad de expresión y a la libertad de expresión en Internet, ya que contemplaba penas de hasta tres años de prisión por ejemplo por difundir a través de Internet información que fuera claramente ofensiva o amenazante. Pero en lo que más nos importa, recogía, entre otras afirmaciones, que "si el derecho a la libertad de expresión incluye el derecho a difundir información al mayor número de población posible, el acceso que permite el ejercicio de ese derecho, es también parte integral de dicho derecho. El más amplio ámbito de circulación de la información o su mayor impacto, no puede restringir el contenido del derecho ni justificar su denegación".

En el plano de los límites, y por su particular actualidad, también hay que hacer mención, tal y como hemos apuntado en el plano normativo, al denominado "discurso de odio" sobre el que la jurisprudencia a uno y otro lado del Atlántico también se ha pronunciado. En este caso cabe subrayar que, debido a la ya resaltada fuerza de la libertad de expresión en Internet, en el caso de Estados Unidos, el discurso del odio solo puede ser un límite a dicha libertad en las más extremas circunstancias, tal y como quedó acreditado en la Sentencia de 22 de

[241] Colombia. Corte Constitucional. Sentencia de 10 de febrero de 2016. Acceso al texto de la Sentencia en el siguiente enlace: http://www.corteconstitucional.gov.co/relatoria/2016/t-050-16.htm
[242] India. Tribunal Supremo. Caso Shreya Singhal v. Union of India. Sentencia de 24 de marzo de 2015. Acceso al texto de la Sentencia en el siguiente enlace: http://supremecourtofindia.nic.in/FileServer/2015-03-24_1427183283.pdf

junio de 1992[243] (caso *R.A.V. v. City of St. Paul*). En referencia a Internet, todavía no se tiene conocimiento de ningún caso que haya llegado al más alto tribunal. Sin embargo sí disponemos ya de una Sentencia de la Corte de Apelación para el Noveno Circuito de 2002 (caso *Planned Parenthood of the Columbia/Willamette, Inc. vs. American Coalition of Life Activists*)[244]. Se trataba de un caso en el que los segundos habían elaborado una serie de posters al modo del "viejo oeste" con los nombres de una docena de doctores que practicaban el aborto y acusándoles de crímenes contra la humanidad. Además, y estos es lo relevante, las fotos se subían a una página web denominada "los archivos de Nuremberg" en la que los referidos doctores aparecían de tres modos distintos: si el doctor estaba vivo la foto estaba en color, si estaba herido la foto estaba en gris, y si estaba muerto entonces estaba tachado. Cuatro de los doctores señalaron que ello constituía una "verdadera amenaza", y el tribunal, aplicando el denominado "test de Brandenburgo" (que hemos citado más arriba) en virtud del cual la libertad de expresión no ampara la que vaya dirigida a incitar o producir inminentes acciones ilegales y que tengan una gran posibilidad de incitar o producir dichas acciones. En definitiva se consideró que el sitio web había sobrepasado los límites de la libertad de expresión, aunque el caso no llegó al Tribunal Supremo.

En el caso de Canadá sin embargo, la jurisprudencia ha sido distinta marcando verdaderos límites a la libertad de expresión. La Sentencia de referencia es la dictada por su Tribunal Supremo de 27 de febrero en el conocido caso *Saskatchewan Human Rights Commission vs. Whatcott*[245] y en el que, a los efectos que nos ocupan, el Tribunal Supremo destacaba que "en términos de divulgación de los mensajes de odio, está hoy el impacto añadido de Internet".

En lo que concierne al conteniente europeo, la doctrina general puede quedar resumida en la STEDH de 6 de julio de 2006 (caso *Erbakan vs Turkey*)[246] en la que se afirmaba que "la

[243] Estados Unidos. Tribunal Supremo. Caso R.A.V. v. City of St. Paul. Sentencia de 22 de junio de 1992. Acceso al texto de la Sentencia en el siguiente enlace: https://www.law.cornell.edu/supremecourt/text/505/377

[244] Estados Unidos. Corte de Apelación del Noveno Circuito. Caso Planned Parenthood of the Columbia/Willamette, Inc. v. American Coalition of Life Activists. Sentencia de 16 de mayo de 2002. Disponible en web: http://www.legalmomentum.org/legal-cases/planned-parenthood-v-american-coalition-life-activists

[245] Canadá. Tribunal Supremo. Caso Saskatchewan Human Rights Commission v Whatcott. Sentencia de 27 de febrero de 2013. Acceso al texto de la Sentencia en el siguiente enlace: https://scc-csc.lexum.com/scc-csc/scc-csc/en/12876/1/document.do

[246] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Primera Sección). Caso Erbakan vs Turkey. Sentencia de 6 de julio de 2006. Acceso al texto de la Sentencia en el siguiente enlace: http://hudoc.echr.coe.int/eng#{"itemid":["001-76232"]}

tolerancia y el respeto por la igual dignidad de todos los seres humanos constituye el fundamento de una sociedad plural y democrática. Siendo esto así, como una cuestión de principio puede considerarse necesario en determinadas sociedades democráticas sancionar o incluso prevenir toda forma expresión que pueda expandir, incitar promover o justificar odio basado en intolerancia…partiendo de que las formalidades, condiciones, restricciones o penas impuestas son proporcionadas al legitimo objetivo perseguido".

Para terminar con nuestra reflexión sobre los límites, no podemos dejar de hacer mención a otra vertiente, ya apuntada, vinculada a la libertad de expresión en Internet: la problemática que plantean algunas medidas jurídicas tradicionales como es en particular la relativa al secuestro de publicaciones. Dos casos acaecidos en Francia y España respectivamente son una muestra clara de las dificultades a las que se enfrentan las viejas instituciones jurídicas.

El primero de estos fue el caso de las historias del doctor Claude Gubler, autor del *libro Le grand secret,* un detallado recuento de la enfermedad de Mitterrand y de los esfuerzos de éste y sus allegados por ocultarla. Tan sólo en el primer día de su publicación en 1995, se vendieron 40,000 ejemplares y la edición del libro causó revuelo en la opinión pública francesa. La familia Mitterrand decidió actuar y acusó a Gubler de violar el secreto médico publicando muchos detalles íntimos. A 24 horas de su aparición, la venta quedó prohibida, veto confirmado por la Corte de Apelaciones de Paris en marzo del año siguiente, cuando ordenó la requisa de los ejemplares que aún estaban distribuidos. Sin embargo, en un cibercafé de Besançon Pascal Barbiaud escaneó la obra completa y la subió a la red donde recibía cerca de 800 visitas al día. El sitio fue clausurado al poco tiempo, pero el archivo sigue estando en línea hasta la fecha, gracias a las incontables copias que de él se hicieron, lo que demostraba la ineficacia del secuestro de la publicación[247]. Cabe subrayar que este caso acabó en el TEDH que el 18 de mayo de 2004[248] dictó una Sentencia condenando a Francia por vulnerar el derecho a la libertad de expresión adoptando una medida de prohibición definitiva desproporcionada y sin que concurriera una necesidad social imperativa.

[247] Para conocer más detalladamente este caso y en general la experiencia francesa respecto a la relación entre Internet y la libertad de expresión, ver MAILLAND, J., Freedom of Speech, the Internet, and the Costs of Control: The French Example, *New York University Journal of International Law & Politics*, Summer 2001, Vol. 33, nº 4, p. 1179-1234.

[248] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Sección Duodécima). Caso Sociéte Plon vs. France. Sentencia de 18 de mayo de 2004. Acceso al texto de la Sentencia en el siguiente enlace:

El segundo de estos casos fue el referido a la publicación por la revista española *El Jueves* de una portada obscena en la que se caricaturizaban a SAR los Príncipes de Asturias. El posible delito de injurias a los descendientes del Rey que contempla el Código Penal español en su art. 491. Estos hechos llevaron al Juzgado Central de Instrucción nº 6 a ordenar el secuestro o retirada de las publicaciones y también el bloqueo del acceso a dicha caricatura en la Web de la revista. Sin embargo, cuando se ordenó está medida, si bien no era accesible a través de dicha Web, sí lo era en multitud de Webs españolas y extranjeras.

En definitiva la ausencia o reducción a lo insignificante de los conceptos de espacio y tiempo en Internet hacen que sea difícil aplicar algunos de los mecanismos jurídicos tradicionales a la libertad de expresión e información en Internet. Sin propugnar el excepcionalismo, lo que resulta una realidad es que, dentro de la tradicional técnica de ponderación de derechos fundamentales se ha de introducir la viralidad en la ecuación. No estamos por tanto hablando de modificar la filosofía subyacente a la citada técnica de ponderación, pero sí de tener en cuenta el cualitativo impacto del factor tecnológico.

3.2.2.4 La necesaria colaboración público-privada en Internet: el régimen de responsabilidad de los PSI

En todo caso, los límites citados se conectan directamente con otro punto al que quería hacer mención en el régimen jurídico de la libertad de expresión en Internet: la responsabilidad por los contenidos, ya que, como afirma la Corte Constitucional de Colombia, en Sentencia de 12 de mayo de 2015[249]: "La libertad de expresión se deriva de que este derecho no solo faculta a las personas para manifestar sus ideas y opiniones, y para transmitir información, sino que también protege que el contenido expresado se difunda y llegue a otros. Así las cosas, imponer responsabilidades a los intermediarios de Internet por los contenidos transmitidos limitaría de forma importante la difusión de ideas por este medio de comunicación, pues les daría el poder para regular el flujo de información en la red". Se trata de una cuestión de enorme relevancia igualmente en la computación en nube, por cuanto veremos más adelante qué papel puede jugar la industria a la hora de flexibilizar el actual

[249] Colombia. Corte Constitucional. Sentencia de 12 de mayo de 2015. Acceso al texto de la Sentencia en el siguiente enlace: http://www.corteconstitucional.gov.co/relatoria/2015/t-277-15.htm

régimen jurídico en caso de que sea necesario para una adecuada regulación del derecho fundamental a la protección de datos.

El ámbito geográfico donde este debate se vive de una manera más intensa es quizá el europeo precisamente porque en el caso norteamericano hace que el debate esté más limitado por la amplitud de su I Enmienda. Y una vez más, va a ser la jurisprudencia la que vaya abriendo el camino en una de las cuestiones de mayor relevancia ante la que nos podemos encontrar.

Efectivamente, uno de los principales protagonistas o actores de la vida en Internet son sin duda los intermediarios: las operadoras de telecomunicaciones, los grandes proveedores de servicios de almacenamiento, los motores de búsqueda...Precisamente su importancia y su labor nuclear hace que su régimen de responsabilidad constituya uno de los elementos de debate más recurrentes en el Derecho de Internet. A este respecto, la Comunicación de la Unión sobre la Estrategia del Mercado Único Digital contempla, entre otros objetivos[250]: la clarificación de las normas aplicables a las actividades de los intermediarios en relación con las obras protegidas por derechos de autor, particularmente por la creciente participación de estos intermediarios en la distribución de contenidos; o en qué medida requerir a los intermediarios para ejercer una mayor responsabilidad y diligencia debida en la manera en que gestionan sus redes y sistemas.

Desde el punto de vista jurídico el régimen de responsabilidad de los proveedores de servicios de intermediación se encuentra principalmente contemplado a día de hoy en 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). En realidad, este sucinto régimen jurídico, que refleja el propio espíritu liberalizador de la Unión Europea en la materia ha dado lugar a numerosos criterios interpretativos, en los que también la referencia a la libertad de expresión ha jugado en ocasiones un importante papel.

[250] UNIÓN EUROPEA. Comunicación de la Comisión Europea sobre la Estrategia de un Mercado Único Digital para Europa, COM(2015) 192 final, Bruselas, 6 de mayo de 2015. Disponible en web: http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf

Una de las primeras dudas que en ocasiones se plantea es respecto al propio concepto de intermediario. A efectos de esta definición, el anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (en adelante LSSI) recoge lo que se puede considerar como servicios de intermediación: la provisión de servicios de acceso a Internet, la transmisión de datos por redes de telecomunicaciones, la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, el alojamiento en los propios servidores de datos, aplicaciones o servicios suministrados por otros y la provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet.

Aunque se pueda pensar que está claro el concepto, en ocasiones las dudas se han planteado en los tribunales. Esto fue por ejemplo lo que ocurrió en el caso del Auto del TJUE de 19 de febrero de 2009 en el marco de un litigio entre *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH* y *Tele2 Telecommunication GmbH*[251]. Con rotundidad –y buena prueba de ello es la utilización del Auto como forma de resolución- el TJUE señaló que un proveedor de acceso que se limita a permitir a un cliente acceder a Internet sin proponer otros servicios ni ejercer un control de Derecho o de hecho sobre el servicio utilizado, presta un servicio que puede ser utilizado por un tercero para infringir un derecho de autor o un derecho afín a los derechos de autor, ya que facilita al usuario la conexión que le permitirá infringir dichos derechos. Por tanto una de las primeras modalidades de servicios de intermediación es la que presta el proveedor de acceso a Internet, que tanto la normativa española como la Directiva comunitaria definen como la prestación de un servicio de la sociedad de la información consistente en transmitir por una red de comunicaciones datos facilitados por el destinatario del servicio, incluyendo el almacenamiento automático, provisional y transitorio de los datos, siempre que sirva exclusivamente para permitir su transmisión por la red de telecomunicaciones y su duración no supere el tiempo razonablemente necesario para ello. Es el protagonista por ejemplo también en la Sentencia del TJUE de 27 de marzo de 2014 (caso *UPC Telekabel Wien*)[252]. Se trataba de un supuesto

[251] Unión Europea. Tribunal de Justicia de la Unión Europea. Caso LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH y Tele2 Telecommunication GmbH. Auto de 19 de febrero de 2009. Acceso al texto del Auto en el siguiente enlace: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd7ef87ac0e8d048da9147d2239b7db0d0.e34KaxiLc3qMb40Rch0SaxuRbNn0?text=&docid=77489&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=61423

[252] Unión Europea. Tribunal de Justicia de la Unión Europea. Caso UPC Telekabel Wien. Sentencia de 27 de marzo de 2014. Acceso al texto de la Sentencia en español en el siguiente enlace: http://curia.europa.eu/juris/document/document.jsf?text=&docid=151622&pageIndex=0&doclang=es&mode=req&dir=&occ=first&part=1&cid=62837

en el que *Constantin Film* y *Wega*, dos productoras cinematográficas, tras comprobar que un sitio de Internet ofrecía, sin su consentimiento, la posibilidad de descargar o de ver en *streaming* algunas de las películas que habían producido, solicitaron del tribunal competente la adopción de medidas cautelares para que se ordenase a *UPC Telekabel*, catalogado como un proveedor de acceso a Internet, bloquear el acceso de sus clientes al sitio de Internet en cuestión. En este caso, el Tribunal de Instancia (*Handelsgericht Wien*) prohibió a *UPC Telekabel* facilitar a sus clientes el acceso al sitio de Internet controvertido y le dijo además cómo hacerlo: bloqueando el nombre de dominio y la dirección IP que en aquel momento tenía dicho sitio web y, cualquier otra dirección IP del mismo del que la citada empresa pudiera tener conocimiento. Frente a dicha resolución, el tribunal de apelación (*Oberlandesgericht Wien)* modificó parcialmente la resolución, matizando que, en lo que respecta a la protección de los derechos de autor, *UPC Telekabel* únicamente podía ser obligada a prohibir a sus clientes el acceso al sitio de Internet controvertido bajo la forma de una obligación de resultado que debía ser libre de elegir los medios para lograr dicho resultado. En referencia a este último pronunciamiento, el TJUE reconoce que restringe la libertad de empresa, pero al mismo tiempo afirma que no parece atentar contra la esencia misma de dicha libertad. Y ello porque un requerimiento judicial como el que es objeto del procedimiento principal permite a su destinatario definir las medidas concretas que hayan de adoptarse para alcanzar el resultado perseguido y le permite eximirse de su responsabilidad demostrando que ha adoptado todas las medidas razonables. En este caso la responsabilidad de estos proveedores está excluida salvo que ellos mismos hayan originado la transmisión, modificado los datos o seleccionado éstos o a los destinatarios de dichos datos; sin que se incluya en el concepto de modificación la manipulación estrictamente técnica de los archivos que alberguen los datos, que tiene lugar durante su transmisión (artículo 14 LSSI y 12 de la Directiva de Comercio Electrónico).

En fin, también en el campo de los proveedores de acceso nos encontramos en el Reino Unido con el caso resuelto por el Alto Tribunal de Justicia de 10 de marzo de 2006 en el caso *Bunt vs. AOL, Tiscalli y BT*[253]*.* Se trataba de un supuesto en el que el Sr. Bunt demandó a tres personas físicas por difamación y acoso por intervenciones realizadas en un chat que consideraba difamadoras. Sin embargo, en lo que ahora nos ocupa, demandó también a tres

[253] Reino Unido. Alto Tribunal de Justicia. Caso Bunt vs. AOL, Tiscalli y BT. Sentencia de 10 de marzo de 2006. Acceso al texto de la Sentencia en inglés en el siguiente enlace: http://www.5rb.com/wp-content/uploads/2013/10/Bunt-v-Tilley-QBD-10-Mar-2006.pdf

proveedores de acceso a Internet sobre la base de que al haber facilitado cada uno de ellos a su respectivo usuario con una conexión, eran también responsables por los comentarios objeto de la demanda. El tribunal rechazó la responsabilidad de estos, considerando que la posición de los PSI no es análoga a la de un distribuidor de material difamatorio. A mayor abundamiento el tribunal señaló que los PSI lo eran en los términos de la normativa de comercio electrónico y que como tales no tenían conocimiento de los comentarios vertidos por los usuarios. Del mismo modo el tribunal afirmó que también el artículo 1 de la Ley inglesa de Difamación de 1996 otorgaba a los PSI una completa defensa en relación con cualquier reclamación respecto a comentarios de los que no se les había dado conocimiento.

Al margen de estos proveedores de acceso, en la normativa comunitaria existen otros dos servicios de intermediación. Por un lado, el denominado "*caching"*, que se da cuando los prestadores de un servicio de intermediación que transmitan por una red de telecomunicaciones datos facilitados por un destinatario del servicio y, con la única finalidad de hacer más eficaz su transmisión ulterior a otros destinatarios que los soliciten, los almacenan en sus sistemas de forma automática, provisional y temporal. En este caso, el régimen de responsabilidad contempla que estará eximido siempre que estemos ante el almacenamiento automático, provisional y temporal de esta información, realizado con la única finalidad de hacer más eficaz la transmisión ulterior de la información a otros destinatarios del servicio, a petición de éstos, y siempre que el PSI no modifique la información; cumpla las condiciones de acceso a la misma; cumpla las normas relativas a la actualización de la información, especificadas de manera ampliamente reconocida y utilizada por el sector; no interfiera en la utilización lícita de tecnología ampliamente reconocida y utilizada por el sector, con el fin de obtener datos sobre la utilización de la información; y servicios actúe con prontitud para retirar la información que haya almacenado, o hacer que el acceso a ella será imposible, en cuanto tenga conocimiento efectivo del hecho de que la información ha sido retirada del lugar de la red en que se encontraba inicialmente, de que se ha imposibilitado el acceso a dicha información o de que un tribunal o una autoridad administrativa ha ordenado retirarla o impedir que se acceda a ella (artículo 15 LSSI y 13 de la Directiva de Comercio Electrónico).

A las dos conductas anteriores se añade lo previsto respecto a la conducta de almacenamiento de datos (hosting) como prevé el artículo 14 de la Directiva de Comercio Electrónico y 16 LSSI, donde se establece igualmente que el PSI no es responsable siempre que no tenga conocimiento efectivo de que la actividad o la información es ilícita; o que, en

cuanto tenga conocimiento, actúe con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible.

En fin, en el caso español, cabe añadir el artículo 17 LSSI donde se contempla de manera similar que los PSI que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no son siempre que no tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o cuando teniéndolo, no actúan con diligencia para suprimir o inutilizar el enlace correspondiente.

Como sustrato común, existen dos cláusulas importantes al referido estatuto jurídico de los PSI. Por un lado, se entiende que el PSI tiene el conocimiento efectivo cuando un órgano competente haya 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 correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse. Por otro lado, existe una importante cláusula. Efectivamente, el artículo 15 de la Directiva recoge que los Estados miembros no impondrán a los PSI una obligación general de supervisar los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas, respecto de los servicios de transmisión, almacenamiento y alojamiento de datos, respectivamente.

3.2.2.4.1 Naturaleza automática, técnica y pasiva

Con independencia de la conducta desarrollada, uno de los primeros elementos para ser catalogado como PSI, es el que sienta el Considerando 42 de la Directiva 2000/31 que recoge que las exenciones de responsabilidad sólo se aplican a aquellos casos en que la actividad del PSI se limite al proceso técnico de explotar y facilitar el acceso a una red de comunicación mediante la cual la información facilitada por terceros es transmitida o almacenada temporalmente, con el fin de hacer que la transmisión sea más eficiente, y siempre que dicha actividad sea de naturaleza meramente técnica, automática y pasiva (adjetivos muy utilizados por la jurisprudencia a la hora de pronunciarse sobre la exención

de responsabilidad), lo que implica que el PSI no tiene conocimiento ni control de la información transmitida o almacenada.

Como apuntábamos, la jurisprudencia ha entrado a tratar esta cuestión de manera muy activa. En la que probablemente ha sido considerada como una Sentencia estrella, la Sentencia del TJUE de 12 de julio de 2011 (Caso *L'Oréal SA vs eBay*)[254] señalaba que para que un PSI quede comprendido en el ámbito de aplicación del artículo 14 de la Directiva 2000/31 (concerniente al alojamiento), es esencial que sea un "prestador intermediario", y que pierde dicha condición cuando, en lugar de limitarse a una prestación neutra de dicho servicio mediante un tratamiento meramente técnico y automático de los datos facilitados por sus clientes, desempeña un papel activo que le permite adquirir conocimiento o control de tales datos. En el caso concreto, el Tribunal señaló que el mero hecho de que el operador de un mercado electrónico (Ebay) almacene en su servidor ofertas de venta, determine las condiciones de su servicio, sea remunerado por él mismo y dé información general a sus clientes, no son causa suficiente para que se le excluya del régimen de exención de responsabilidad. Sin embargo, dentro de este análisis casuístico, en la misma Sentencia, el TJUE señala que cuando, por el contrario, el PSI presta una asistencia consistente, entre otras cosas, en optimizar la presentación de las ofertas de venta en cuestión o en promover tales ofertas, cabe considerar que no ha ocupado una posición neutra entre el cliente vendedor correspondiente y los potenciales compradores, sino que ha desempeñado un papel activo que le permite adquirir conocimiento o control de los datos relativos a esas ofertas. En este mismo sentido y de manera muy clara, la Sentencia del Tribunal de Apelación de Leeuwarden de 22 de mayo de 2012 (caso *Stokke vs. Marktplaats)*[255] en la que se señaló que la plataforma no era responsable, aunque la plataforma ofreciera servicios de almacenamiento sofisticados. Para esa exención de responsabilidad, el Tribunal se basó en importantes factores tales como que la plataforma tuviera una política de notificación y retirada apropiada; que por sí misma no había causado ningún daño, sino que es simplemente instrumental a la infracción secundaria; el hecho de que, como mucho, tuviera algunas ventajas indirectas derivadas de la infracción; y el hecho de que la infracción tuvo

[254] Unión Europea. Tribunal de Justicia de la Unión Europea. Caso L'Oreal SA vs eBay. Sentencia de 12 de julio de 2011. Acceso al texto de la Sentencia en español en el siguiente enlace: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30ddbacdc0b0d78b4fc49b85d639b1b0c6d6.e34KaxiLc3qMb40Rch0SaxuRbNn0?text=&docid=107261&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=375313

[255] Holanda. Tribunal de Apelación de Leeuwarden de 22 de mayo de 2012. Caso Stokke vs. Marktplaats. Sentencia del 22 de mayo de 2012. Acceso al texto de la sentencia en holandés en el siguiente enlace: http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHLEE:2012:BW6296

lugar en el ámbito del comercio electrónico y de que la adopción de medidas drásticas de cara a prevenir infracciones en este ámbito no es algo obvio[256].

De similar manera, el Tribunal de Casación de París de 17 de febrero de 2011 (caso *Société Nord-Ouest & UGC Images vs Dailymotion*) [257] señaló que el servicio facilitado por *Dailymotion*, una plataforma de videos francesa, era esencialmente pasivo por cuanto no tomaba parte en la actividad de subir y bajar el material audiovisual ni participaba en el contenido y elección de los videos. Igualmente subrayaba que la recodificación, el formateo y la organización de videos eran operaciones técnicas que no ponen de manifiesto ninguna decisión editorial, y que la explotación comercial de la web a partir de la venta de espacios de publicidad no habilitaba a *Dailymotion* para intervenir en los materiales puestos online. De similar manera en cuanto a la no consideración como editor, la Sentencia del Tribunal de Gran Instancia de París de fecha 29 de mayo de 2012 (caso *TF1, TF1 Video, TF1 droits audiovisuels, LCI* y *e-TF1* vs Youtube)[258] se remitía a la doctrina sentada en la Sentencia anterior y en la disquisición respecto a considerar a Youtube como proveedor de servicios de almacenamiento o un editor de contenidos, señalaba que, a pesar de que Youtube ofrece en su sitio web una multitud de facilidades diseñadas para ayudar a los usuarios a encontrar los videos, no determina el contenido del material subido y por tanto no es un editor que le haga perder la condición de PSI. Y del mismo modo se subrayaba que no hay intervención manual por parte de YouTube, sino que la función de "videos relacionados" tiene una organización automática basada en algoritmos. En fin, al igual que en el caso *Dailymotion*, también el debate sobre los espacios de publicidad surgió en esta Sentencia, negando el Tribunal que el hecho de que Youtube incluya anuncios pueda servir para calificarlo como editor. En tanto la publicidad no determina el contenido, nada prohíbe a un proveedor de servicios de almacenamiento obtener ingresos derivados de la publicidad. Además, el tribunal también se pronunciaba respecto a la retirada del contenido una vez notificada la existencia del mismo. Señalaba que Youtube tenía la obligación de retirar el contenido o

[256] ANTIC, M., LAGEMAAT, A., VAN DER SLOOT, B., y VAN STEKELENBURG, M., Dutch National Report, *International League of Competition Law (LIDC),* Congress, Oxford, 22-24/September/2012, http://www.ligue.org/uploads/documents/rpportBNL.pdf

[257] Francia. Tribunal de Casación de París. Caso Société Nord-Ouest & UGC Images vs Dailymotion. Sentencia de 17 de febrero de 2011. Acceso al texto de la Sentencia en francés en el siguiente enlace: http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000023607266&fastReqId=194051815&fastPos=1

[258] Francia. Tribunal de Gran Instancia de París. caso TF1, TF1 Video, TF1 droits audiovisuels, LCI y e-TF1 vs Youtube. Sentencia de 29 de mayo de 2012. Acceso al texto de la Sentencia en francés en el siguiente enlace: https://es.scribd.com/doc/95145955/Youtube-TF1-Jugement-29-Mai-2012#download&from_embed

impedir el acceso a la mayor brevedad posible (*promptly*), concepto este que no es objeto de definición por la legislación francesa. Sin embargo, en el caso concreto, los jueces sí que consideraron que la retirada cinco días después no era razonable.

En España el debate más vivo sobre esta cuestión surgió quizá con la conocida como Sentencia Telecinco vs. Youtube dictada por la Audiencia Provincial de Madrid el 14 de enero de 2014[259]. Se trataba de un recurso de apelación que enfrentaba a Youtube con Telecinco por una demanda de infracción de derechos de propiedad intelectual. En este caso Telecinco planteó que Youtube no llevaba a cabo una actividad de naturaleza meramente técnica, automática y pasiva porque suscribía contratos con entidades de gestión, establece política de contenidos que impone a los usuarios, incluye en los términos de uso de una licencia de uso y por sus labores editoriales y de control sobre los contenidos almacenados. La Audiencia Provincial dio respuesta a cada una de las cuestiones planteadas y señaló que la adquisición de licencias globales no entraña conocimiento o control, que las licencias de uso en los TOU, precisamente refuerza su condición de intermediarios, que la política de contenidos son condiciones de servicio cuya fijación no excluye del régimen de responsabilidad previsto en la Directiva, y que las labores de catalogación vienen en gran medida predeterminadas por los usuarios y el rol proactivo es en un número muy pequeño de contenidos.

Más recientemente, y en línea similar, el Tribunal de Apelación de Milán, en su Sentencia de 7 de enero de 2015[260] se enfrentó en apelación a un caso similar. Se trataba de un supuesto que enfrentaba a RETI, el mayor grupo privado de televisión en Italia; con Yahoo, plataforma que aloja también videos. En concreto, en 2008, la RETI italiana demandó a Yahoo por la presencia de muchos videos de la cadena en la plataforma de Yahoo. En instancia, el Tribunal de instancia en Milán en 2011 resolvió una sentencia en la que declaraba a Yahoo culpable por infracción de la propiedad intelectual debido a su papel como proveedor de almacenamiento activo y consiguientemente la imposibilidad de aplicar la Directiva de Comercio electrónico. Yahoo no se podía beneficiar del régimen de responsabilidad de la

[259] España. Audiencia Provincial de Madrid. Caso Telecinco vs. Youtube. Sentencia de 14 de enero de 2014. Acceso al texto de la Sentencia en el siguiente enlace: http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=6955036&links=pssis&optimize=20140210&publicinterface=true

[260] Italia. Tribunal de Apelación de Milán. Caso RETI vs. Yahoo. Sentencia de 7 de enero de 2015. Acceso al texto de la Sentencia en italiano en el siguiente enlace: http://www.ricercagiuridica.com/sentenze/sentenza.php?num=4458

Directiva aplicable a los proveedores pasivos solamente. El Tribunal consideró a Yahoo un prestador activo por una serie de motivos: un sistema de denuncias de abuso, cuya existencia indicaría que Yahoo asume un control de la legalidad del material publicado; la existencia de funcionalidades internas como un motor de búsqueda y un botón para informar de los videos relacionados, consistente en una función de indexación automática; y la licencia otorgada a Yahoo por los usuarios sobre el contenido subido. El Tribunal de Apelación de Milán rechazó dicho argumento en su Sentencia de 7 de enero de 2015 y de hecho subrayó que las tecnologías actuales no son per se suficientes para hacer activos los servicios ofrecidos por un proveedor de almacenamiento, con independencia de las técnicas utilizadas para gestionar la subida de contenidos y del interés del proveedor por perseguir ganancias económicas. De hecho señala que esa distinción no se encuentra en la Directiva de Comercio electrónico y la jurisprudencia del TJUE clarifica que una actividad de indexación automática (C-324/09, L'Oreal vs. eBay) no es suficiente para romper la neutralidad y pasividad. En definitiva, afirma que los elementos tenidos en cuenta por el tribunal de primera instancia no son suficientes para excluir a Yahoo del régimen de responsabilidad de la Directiva. Como primera conclusión por tanto en este punto podemos reseñar que es necesario analizar en cada caso concreto para observar si las conductas llevadas a cabo por el PSI son suficientes para desvirtuar la naturaleza activa y neutral; y cabe añadir que existe una jurisprudencia relativamente consolidada en cuanto a que determinadas conductas no implican que se desvirtúe dicha naturaleza. Así, usar sistemas de valoración es una característica habitualmente usada por este tipo de plataformas de intermediación y suelen estar basadas en un sistema automático, pasivo y neutral; y lo mismo ocurre con las garantías de usuarios. O por ejemplo, la recepción o facilitación del pago entre usuarios, lo cual no tiene un impacto en la neutralidad de los servicios de almacenamiento facilitados por una plataforma. Las funcionalidades técnicas de muchas de las plataformas no son elementos suficientes para quebrar su neutralidad y pasividad

3.2.2.4.2 La no obligación general de supervisión.

Pero en línea con lo anterior e íntimamente conectado con lo dicho, está la cláusula de cierre a la que hemos hecho mención anteriormente en el artículo 15 en el que se decía que los Estados miembros no impondrán a los PSI una obligación general de supervisar los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de

hechos o circunstancias que indiquen actividades ilícitas, respecto de los servicios de transmisión, almacenamiento y alojamiento de datos, respectivamente. La jurisprudencia ha tenido ocasión en varias ocasiones y en algunas de las sentencias citadas, respecto a la imposibilidad de establecer sobre el PSI esa obligación general de supervisión. Así se pronunció el TJUE en la Sentencia de 24 de noviembre de 2011, en el caso *Sabam vs. Scarlet*[261]. Nos encontramos ante un conocido caso en el que, por un lado, Sabam es una sociedad de gestión que representa a los autores, compositores y editores de obras musicales, autorizando el uso por terceros de sus obras protegidas; y por otro Scarlet es un proveedor de acceso a Internet que proporciona a sus clientes acceso a Internet, sin ofrecer otros servicios como la descarga o el intercambio de archivos. Los motivos de traer a colación este caso es que mediante diligencia de 24 de junio de 2004, Scarlet fue citada ante el Presidente del tribunal de primera instancia de Bruselas a petición de Sabam, que alegó que Scarlet, en su condición de PAI, estaba en la mejor situación para adoptar medidas dirigidas al cese de las infracciones de derechos de autor cometidas por sus clientes; y solicitó, en primer lugar, que se declarase la existencia de infracciones de los derechos de autor sobre las obras musicales pertenecientes a su repertorio, en particular del derecho de reproducción y del derecho de comunicación al público, como consecuencia del intercambio no autorizado de archivos electrónicos musicales realizado gracias a programas «peer to peer», infracciones cometidas a través de la utilización de los servicios de Scarlet; pero además, en lo que ahora importa, solicitó que se condenara a Scarlet a poner fin a dichas infracciones, impidiendo o bloqueando cualquier forma de envío o de recepción por sus clientes de archivos que reproduzcan una obra musical sin autorización de sus titulares mediante un programa «peer to peer», con apercibimiento de multa coercitiva. Scarlet recurrió con base en argumentos fácticos y técnicos, por un lado; pero sobre todo con base en argumentos jurídicos. Efectivamente, por un lado, Scarlet recurrió dicha resolución en apelación ante el órgano jurisdiccional remitente, alegando, en primer lugar, que le resultaba imposible dar cumplimiento al citado requerimiento judicial porque no están demostradas la eficacia ni la perennidad de los sistemas de bloqueo o filtrado y porque el establecimiento de tales dispositivos tropieza con numerosos obstáculos prácticos, como por ejemplo problemas relativos a la capacidad de la red o al impacto en ésta; pero por otro lado Scarlet alegó que

[261] Unión Europea. Tribunal de Justicia de la Unión Europea. Caso Sabam vs. Scarlet. Sentencia de 24 de noviembre de 2011. Acceso al texto de la Sentencia en español en el siguiente enlace: http://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=21155

el citado requerimiento judicial no era conforme con el artículo 21 de la Ley de 11 de marzo de 2003 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, que transpone al Derecho nacional el artículo 15 de la Directiva 2000/31, puesto que le imponía de hecho una obligación general de supervisar las comunicaciones en su red, ya que cualquier dispositivo de bloqueo o de filtrado del tráfico «peer-to-peer» requería necesariamente una supervisión generalizada de todas las comunicaciones que pasaban por esa red. En realidad, un sistema de filtrado como el que solicitaba la entidad de gestión y respaldó el tribunal de instancia, que el PAI identifique: de entre el conjunto de las comunicaciones electrónicas de todos sus clientes, los archivos correspondientes al tráfico «peer-to-peer»; en el ámbito de dicho tráfico, los archivos que contuvieran obras sobre las que los titulares de derechos de propiedad intelectual tengan supuestamente derechos; cuáles de esos archivos se intercambiaban de un modo ilícito; y la necesidad de bloquear los intercambios de archivos que considere ilícitos. Esta supervisión preventiva exigía una vigilancia activa de la totalidad de las comunicaciones electrónicas efectuadas en la red del PAI afectado y, por lo tanto, hubiera comprendido todos los datos que se vayan a transmitir y todos los clientes que utilicen dicha red. Es decir, el citado requerimiento judicial impondría a dicho PAI una supervisión general prohibida por el artículo 15, apartado 1, de la Directiva 2000/31.

Algunas de las sentencias anteriormente citadas también recogen de manera rotunda esta doctrina. Así, la Sentencia de la Audiencia Provincial de Madrid antes mencionada, concluye que no se puede imponer a las plataformas la obligación de supervisión o control de los contenidos de los usuarios. De hecho, en este caso, la empresa Telecinco argumentaba que la prohibición de una obligación de supervisión general no excluye la obligación de supervisión en casos específicos y se basaba en aspectos como la utilización de la “mosca” de Tele5 es suficiente a efectos de poder constatar la ilicitud y que, para la retirada de contenidos, basta una notificación general y no de manera individualizada y concreta. Y es en referencia a este último punto la Audiencia señaló que precisamente la falta de precisión en la identificación de los contenidos concretos conllevaba se estaría imponiendo, de facto, una obligación de supervisión activa de los contenidos alojados en la plataforma, obligación proscrita por el artículo 15 de la Directiva de Comercio Electrónico. En esencia, esta Sentencia confirmaba que YouTube es un prestador de servicios de intermediación que se beneficia de un régimen de responsabilidad especial que le exime de tener que vigilar o filtrar activamente los vídeos que suban los usuarios, que las notificaciones de carácter genérico enviadas por Telecinco a YouTube no sirven para activar la responsabilidad de YouTube y

que, de atender las solicitudes genéricas de retirada formuladas por Telecinco, dada la falta de precisión en la identificación de los contenidos concretos, se estaría imponiendo, de facto, una obligación de supervisión activa de los contenidos alojados en la plataforma, obligación proscrita por el artículo 15 de la Directiva de Comercio Electrónico. Esta postura fue ratificada de manera muy similar por el Tribunal de apelación de Milán en enero de 2015 que incide en que de cara a remover el contenido ilícito por parte del proveedor, dicho contenido debe ser específicamente identificado, lo que conlleva que es necesario que expresamente se indique la URL, no siendo suficiente con un aviso general que recoja únicamente el título de los programas.

3.2.2.4.3 El concepto de conocimiento efectivo

Tal y como ya se ha podido ver, uno de los conceptos clave en los que se basa el régimen jurídico de los PSI y a partir de los cuales surge el concepto de responsabilidad, es el de conocimiento efectivo. En concreto en el caso del alojamiento el artículo 16 señala que los prestadores de un servicio de intermediación consistente en albergar datos proporcionados por el destinatario de este servicio no serán responsables por la información almacenada a petición del destinatario, siempre que no tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos. A efectos de considerar cuándo tiene el conocimiento efectivo se dará cuando un órgano competente haya 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 correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse. En la misma línea, el artículo 17, referido a los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda les exime de responsabilidad siempre que no tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o; si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente; entendiéndose igualmente que tiene el conocimiento efectivo a que se refiere el párrafo cuando un órgano competente haya 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 correspondiente resolución, sin perjuicio

de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse. Como dice la Sentencia de la Audiencia Provincial de Madrid de 20 de diciembre de 2005[262], el legislador español, con el fin de no menoscabar el ejercicio del derecho a la libertad de expresión y otros valores, ha optado por la no obligación de fiscalizar los contenidos por parte de los prestadores de servicios, si bien les impone un deber de diligencia…con base además de que es imposible controlar el enorme volumen de información que se introduce en los PSI.

Como no podía ser de otra manera, también aquí la labor jurisprudencial ha sido clave, existiendo en España una jurisprudencia que, como vamos a ver, tiene un cierto componente pendular. Así, en la Sentencia de instancia que fue objeto de apelación resuelto por la Sentencia citada en el párrafo anterior, el Tribunal señaló que la demandada advirtió al propietario de la página, a través de un comunicado en la misma, que habían recibido una carta notarial por la publicación de documentos posiblemente atentatorios contra el honor; y razonó que el artículo 16 de la Ley 34/02, de 11 de julio, no dejaba lugar a duda sobre la exención de responsabilidad de la demandada en el presente supuesto, al no existir previa declaración por el órgano competente de la ilicitud del contenido de la página web ordenando su retirada o imposibilitando el acceso a la misma, ni de la existencia de la lesión al derecho fundamental al honor del actor. En conclusión, el Tribunal señalaba que no bastaba con el requerimiento notarial, sino que era necesario, y esto es lo relevante, una resolución de un órgano competente.

No obstante, este pronunciamiento que podemos catalogar como formalista, y que se vio ratificado por posteriores sentencias por parte de nuestra jurisprudencia, se vio modificado como consecuencia de la Sentencia del Tribunal Supremo de 9 de diciembre de 2009, conocida como caso Putasgae[263]. Se trataba de un supuesto en el que una asociación prestaba un conjunto de servicios entre los que se incluía el alojamiento de determinadas direcciones entre las cuales se encontraban algunas que contenían afirmaciones injuriosas

[262] España. Audiencia Provincial (Sección 14). Sentencia de 20 de diciembre de 2005. El acceso a la sentencia completa en el siguiente enlace: http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=957378&links=2807937014200510067 9&optimize=20060216&publicinterface=true

[263] España. Tribunal Supremo (Sala de lo Civil). Sentencia 773/2009 de 9 de diciembre de 2009. Acceso al texto de la sentencia en el siguiente enlace: http://www.internautas.org/archivos/pdf/sentenciasupremoputasgae.pdf

para con la citada entidad de gestión. Las alegaciones presentadas por la Asociación, que había sido declarada responsable en las instancias inferiores, se basaban, conforme a la jurisprudencia antes apuntada, en que no había participado en la elaboración y en la selección de los contenidos y en que carecía del conocimiento efectivo de las afirmaciones allí vertidas. Y es aquí donde el Tribunal Supremo dio un giro a su interpretación y señaló que no cabía una interpretación reduccionista del conocimiento efectivo, máxime por la cláusula "…y de otros medios de conocimiento efectivo que pudieran establecerse". De hecho, el TS subraya que el conocimiento efectivo se obtiene por el prestador del servicio a partir de hechos o circunstancias aptos para posibilitar, aunque mediatamente, o por injerencias lógicas al alcance de cualquiera, una efectiva aprehensión de la realidad de que se trate. El TS en concreto confirmó el criterio del tribunal de apelación que atribuyó ese valor revelador al domino www.putasgae.org dirigido por la "Plataforma de coordinación de movilizaciones contra la SGAE", dirección que la Asociación recurrente le había proporcionado. Consideró que tal título, por el carácter insultante, era un medio adecuado, *ex re ipsa*, para revelar, junto con las circunstancias concurrentes (en especial la realidad de un conflicto entre dicha proveedora de contenidos y la entidad de gestión) conocido por la recurrente, el tenor injurioso de los datos alojados.

A pesar de este giro jurisprudencial, que respondía en gran medida a la realidad de los hechos, pero que fijaba muchas líneas grises, la situación no quedaba clara. Prueba de ello es que en la Sentencia del Tribunal Supremo de 18 de mayo de 2010[264], conocido como caso "quejasonline". Se trataba de un supuesto en el que una persona suplantó al abogado de una empresa utilizando su nombre para verter contenidos críticos con la citada empresa. Se solicitó de la web que alojaba dicho comentario para que lo retiraran y le comunicara el nombre del remitente. A lo primero el titular de la web accedió inmediatamente, y no así a lo segundo. En este caso el tribunal de instancia, así como la Audiencia Provincial, condenaron a la página web a difundir el fallo de la sentencia y satisfacer una cantidad en concepto de indemnización. Sin embargo, el Tribunal Supremo apunta que no se puede condenar a quien aloja contenidos cuando no tengan conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito y, en el caso de que tuvieran dicho

[264] España. Tribunal Supremo (Sala de lo Civil). Sentencia 316/2010, de 18 de mayo de 2010. El acceso a la sentencia completa en el siguiente enlace: http://estaticos.elmundo.es/documentos/2010/05/21/sentencia_foro.pdf

conocimiento, cosa que ocurre, cuando actúen con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible.

De nuevo en esa jurisprudencia pendular, la Sentencia del Tribunal Supremo de 10 de febrero de 2011[265] condenó al titular de la página web en el caso “alasbarricadas.org”. Nos encontramos ante la publicación de graves expresiones atentatorias -según el demandante- contra su honor en la página web "alasbarricadas.org", en el denominado "Foro Anarquista para el debate y contacto directo entre compañer@s", dentro del apartado "El Rey del Pollo Frito. Ramoncín”. Los tribunales de primera y segunda instancia condenaron al responsable del prestador de servicios de alojamiento a eliminar del sitio web las expresiones y fotografías que consideraba atentatorias contra el derecho al honor; a la publicación a su costa de la sentencia; y a abonar, en concepto de indemnización, la cantidad de seis mil euros. En este caso la Sentencia del Tribunal Supremo giró de nuevo en torno al conocimiento efectivo. En el caso concreto el Tribunal señalaba que la web objeto de litigio ofrece un servicio de puesta a disposición para que los consumidores y usuarios alojen sus opiniones en el servidor, sin que el intermediario participara en absoluto en la selección, diseño u organización de dicha información, ni la asumiera, sino que son terceras personas las que vierten esos comentarios. Se recuerda en el argumentario que la exención de responsabilidad cede cuando el intermediario adquiere "conocimiento efectivo" de que la actividad o información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización y no procede a retirar los datos en cuestión. Aquí el demandado recurrió en primer lugar al recordar las dos interpretaciones respecto a qué se debe entender por conocimiento efectivo marcadas por la jurisprudencia anteriormente subrayada, es decir, la existencia de una interpretación estricta, que introduce una lista cerrada de causas de conocimiento; y la más amplia, basada en que el último párrafo del artículo 16.2 contiene una lista meramente ejemplificativa o abierta de supuestos de conocimiento efectivo, pero a la que es susceptible de incorporarse otros elementos. El recurrente, prestador de servicios de alojamiento, alegó para negar el conocimiento efectivo, que no tenía conocimiento de la presunta ilicitud del contenido albergado en la web hasta que no recibió la demanda origen del presente procedimiento, que procedió a retirar inmediatamente el hilo del foro que motivaba la queja tan pronto recibió la demanda y que no existía relación de dependencia laboral,

[265] España. Tribunal Supremo (Sala de lo Civil). Sentencia 72/2011, de 10 de febrero de 2011. El acceso a la sentencia completa en el siguiente enlace: http://s.libertaddigital.com/doc/sentencia-del-supremo-que-condena-a-la-web-alasbarricadas-a-indemnizar-a-ramoncin-41912140.pdf

administrativa o familiar entre el prestatario del servicio y el intermediario, ni contrato de obra o arrendamiento de servicios en el que el prestador intermediario se hubiera reservado expresamente las funciones de dirección o control. El Tribunal Supremo señaló en este caso, con base en la anteriormente citada Sentencia de 9 de diciembre de 2009, que la interpretación estricta no es conforme a la Directiva, por cuanto reduce injustificadamente las posibilidades de obtención del "conocimiento efectivo" de la ilicitud de los contenidos almacenados y amplía correlativamente el ámbito de la exención, en relación con los términos de la norma armonizadora, que exige un efectivo conocimiento, pero sin restringir los instrumentos aptos para alcanzarlo. Afirma que la Directiva atribuye igual valor que al "conocimiento efectivo" a aquel que se obtiene por el prestador del servicio a partir de hechos o circunstancias aptos para posibilitar, aunque mediatamente o por inferencias lógicas al alcance de cualquiera, una efectiva aprehensión de la realidad de que se trate. Y en definitiva confirma el criterio de las sentencias de instancia al señalar que se atribuye ese mismo valor revelador a los contenidos almacenados o enlazados por cuanto su ilicitud es patente y evidente por sí sola, al no depender de datos o información que no se encuentren a disposición del intermediario. Considera que tanto la foto como las expresiones empleadas constituyen una intromisión en el derecho al honor del demandante notoria y manifiesta , y que no era precisa resolución judicial que declarase la ilicitud del contenido de las mismas.

En la misma línea, se sitúa la Sentencia del Tribunal Supremo de 26 de febrero de 2013[266]. Se trataba de un supuesto en el que una persona formuló demanda de protección del derecho al honor contra Editorial Ecoprensa, S.A. como consecuencia de los comentarios y las opiniones vertidas en el foro de la edición digital de un periódico propiedad de dicha editorial. En concreto, solicitaba su retirada, la publicación de la sentencia en dicha página de Internet y una indemnización de veinte mil euros. En este caso, el juzgado de instancia estimó parcialmente la demanda porque si bien no quedó acreditado que el demandado tuviera conocimiento efectivo previo de las expresiones vertidas en su foro y atentatorias al derecho al honor del demandante, no agotó la diligencia que le era exigible como tal creador y administrador de dicho foro para tener un conocimiento efectivo a posteriori, a pesar de que el demandante a través de los servicios jurídicos de la SGAE envió a dicho medio un burofax el día 2 de octubre de 2008 a través del que se le requería la retirada de tales

[266] España. Tribunal Supremo (Sala de lo Civil). Sentencia 128/2013, de 26 de febrero de 2013. Acceso al texto completo de la Sentencia en el siguiente enlace: http://portaljuridico.lexnova.es/jurisprudencia/JURIDICO/195962/sentencia-ts-128-2013-sala-1-de-26-de-febrero-derecho-al-honor-comentarios-ofensivos-insertos

comentarios ofensivos y dicho burofax fue rehusado por la demandada. En concreto la Sentencia de instancia señaló que la editora no agotó la diligencia que le era exigible como tal creador y administrador de dicho foro, pues si bien en su página de Internet se recogen los datos para ponerse en contacto con ella, la advertencia de que las personas que accedan al mismo tienen que identificarse, impidió que el actor pudiera contactar con él y alertarle de las mismas y así ejercer el control a posteriori, retirándolas de inmediato, al rehusar el burofax enviado por el actor por lo que procedió a declarar su responsabilidad. En una postura de vaivén jurisprudencial a la que ya estamos acostumbrados, la Audiencia Provincial de Madrid estimó el recurso de la editorial afirmando que el envío de un burofax y su rechazo por la demandada no son suficientes para justificar la falta de diligencia de esta en la retirada de los comentarios ofensivos, y ello por un triple motivo: porque se trata de un burofax en el que no aparece como remitente el demandante, por el hecho de que el burofax proviniese de los servicios jurídicos de la SGAE y el demandante hubiese sido vocal de dicho organismo no tiene por qué exigir que la demandada estuviera obligada a conocer que la misiva contenía un requerimiento del demandante, y porque aun en el hipotético caso de que se hubiese probado que el burofax hubiese llegado a conocimiento de la demandada y que su contenido era el mismo que el de la carta acompañada a la demanda, de su contenido no se puede determinar qué comentarios eran ofensivos y debían ser retirados. Sin embargo, el Tribunal Supremo volvió a los criterios del juzgado de primera instancia con base, una vez más, en el criterio interpretativo seguido en cuanto al concepto de conocimiento efectivo. En concreto afirmaba que la Audiencia Provincial redujo extremadamente las posibilidades de obtención de dicho conocimiento. Afirmaba que el contenido de lo almacenado en sí mismo es tan revelador que su ilicitud es patente y evidente por sí sola sin necesidad de resolución judicial que así lo declare, así como que el titular de la página web no actuó con la diligencia mínima necesaria para retirar los contenidos lesivos pese a que las características del foro lo aconsejaban, llegando incluso a rehusar el envío de un burofax remitido por el demandante. En definitiva, el Tribunal Supremo lleva a cabo una equiparación o una inclusión en el concepto de conocimiento efectivo, de los supuestos en que el contenido y naturaleza de los mensajes alojados tuvieran una naturaleza sumamente grave y son claramente ofensivos del honor. Además, señalaba que en este caso no cabía alegar desconocimiento por parte de la entidad demandada a raíz del fax recibido, dado que en él se advertía con claridad la existencia de comunicaciones lesivas del derecho al honor y se reclamaba su retirada, hecho que respondía a la realidad y que impide que el titular de la página web pueda a partir de ese momento desconocer.

En el caso de la Sentencia del Tribunal Supremo de 4 de marzo de 2013[267], nos encontramos con un supuesto que ya no se entronca en un PSI de alojamiento, sino en el supuesto previsto en el artículo 17, es decir, los prestadores de servicios de la sociedad de la información que facilitan enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenido. En este caso se trataba de la demanda de protección de su honor interpuesta por un conocido periodista contra Google Inc. y contra su director ejecutivo, D. Eric E. Schmidt, por la contribución de los demandados en la difusión en la web de artículos en los que se le implicaba con la denominada Operación Malaya. En el tribunal de instancia se negó la responsabilidad del buscador con base en una interpretación estricta al señalar que no existía resolución de órgano competente que declarara la ilicitud de la información y, por tanto, no tenía conocimiento efectivo de la misma. En uno de los casos, ya que eran tres los medios afectados, el juzgado señalaba que el buscador no tenía conocimiento de que la titular de la página había reconocido haber atentado contra el honor del demandante mediante acuerdo transaccional en un procedimiento judicial; mientras que en las otras dos publicaciones digitales, se declaró que no constaba resolución declarando la ilicitud de las publicaciones con lo cual no le era exigible al buscador ninguna diligencia para retirar la información. Precisamente en la Sentencia de la Audiencia Provincial de Madrid, y en referencia al primero de los medios, se señaló que el buscador no había actuado de forma negligente al no retirar los contenidos, ante las comunicaciones remitidas por el demandante, pues si bien en una de estas se le comunicaba la existencia de un procedimiento judicial en el que se había dictado una resolución, no constaba la remisión de la copia de esta resolución, hecho que la Audiencia Provincial valora como suficiente para entender cumplido la falta del requisito legal de conocimiento efectivo de la ilicitud de la información. El Tribunal Supremo además entra en la valoración de la interpretación amplia del concepto de conocimiento efectivo, pero para negar su concurrencia ya que señala que de los hechos acreditados no puede inferirse de forma lógica, al alcance de cualquiera, que la información era falsa ni tampoco que se revelara de su contenido su carácter ilícito, supuesto en el que esta Sala ha declarado en otros casos la existencia de conocimiento efectivo. Y añadía que la circunstancia de que la persona que se consideraba ofendida se hubiera dirigido a Google para la retirada de la información por considerarla ilícita no es suficiente para que se produzca esta conducta,

[267] España. Tribunal Supremo (Sala de lo Civil). Sentencia 144/2013, de 4 de marzo de 2013. Acceso al texto de la Sentencia en el siguiente enlace:

cuando, insistía, la información por sí misma tampoco revelaba de manera notoria su carácter ilícito.

Tal y como ya se ha visto, no solamente la jurisprudencia española se ha pronunciado sobre estas cuestiones. Buena prueba es la Sentencia del Tribunal Europeo de Derechos Humanos de 10 de octubre de 2013[268], caso Delfi AS vs. Estonia. En este caso, el 24 de enero de 2006, Delfi publicó un artículo sobre la destrucción accidental de un camino de hielo que unía el continente con unas islas (Saaremaa, Hiiumaa y Muhu) muy visitadas por los turistas locales en invierno. Debido a la rotura, este camino -evidentemente más barato de transitar que los servicios de ferry- se tornó intransitable durante varias semanas. Muchos lectores realizaron mensajes ofensivos (unos 20) y amenazantes en contra del operador del ferry y el propietario. El agraviado solicitó la retirada de los comentarios insultantes y el pago de una indemnización. El portal retiró los comentarios el mismo día de la notificación. Sin embargo, se negó a realizar el pago. Al margen de los límites a la libertad de expresión, en lo que ahora ocupa, esto es, la responsabilidad de los PSI, la cuestión principal de la sentencia es si los portales que alojan foros tienen la consideración de intermediarios de servicios de la sociedad de la información, en cuyo caso se beneficiarían de la exención de responsabilidad de la Directiva de Comercio Electrónico; o si, por el contrario, tienen la naturaleza de proveedores de contenidos, en cuyo caso tienen la obligación de controlar los contenidos. El Tribunal Supremo de Estonia consideró que el portal de noticias tenía la consideración de editor y, por tanto, culpa in vigilando por los contenidos.

En el marco de la jurisprudencia comunitaria, y también en relación con un medio de comunicación, lo cual no es una cuestión menor, conviene analizar la Sentencia TJUE de 11 de septiembre de 2014[269]. En este caso el Sr. Papasavvas solicitaba la reparación del daño que le ocasionaron los artículos publicados en el periódico de tirada nacional O Filelefthеros (Chipre), el 7 de noviembre de 2010, que se pusieron en línea en dos páginas de Internet. Solicitaba también al órgano jurisdiccional nacional que adoptase las medidas provisionales para prohibir la publicación de los artículos controvertidos. Acabamos de decir que la consideración de medio de comunicación tiene su relevancia, y es que el Tribunal de

[268] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Gran Sala). Caso Delfi vs. Estonia. Sentencia de 16 de junio de 2015. Acceso al texto de la Sentencia en inglés el siguiente enlace: http://hudoc.echr.coe.int/eng#{"itemid":["001-155105"]}

[269] Unión Europea. Tribunal de Justicia de la Unión Europea (Sala Séptima). Caso Sotiris Papasavvas vs. O Filelefthеros Dimosia Etaireia. Sentencia de 11 de septiembre de 2014. Acceso al texto de la Sentencia en el siguiente enlace: http://curia.europa.eu/juris/document/document.jsf?docid=157524&doclang=ES

Luxemburgo señalaba que como una sociedad editora de prensa que publica en su página de Internet la versión digital de un periódico tiene conocimiento, en principio, de la información que publica y ejerce un control sobre ésta, no puede ser considerada un prestador de servicios intermediarios, en el sentido de los artículos 12 a 14 de la Directiva 2000/31, con independencia de que el acceso a la página sea de pago o gratuito.

3.2.2.4.4 Un campo de particular controversia: el denominado derecho al olvido

Al margen de la doctrina general anteriormente sentada, existen determinados campos de conflicto en el ámbito del Derecho de Internet que tienen particular interés respecto a la posición que ocupan los prestadores de servicios de intermediación. En concreto ya hemos hecho alguna mención, en el marco de la no obligación general de supervisión, al ámbito de la propiedad intelectual. La segunda cuestión, y que en mucha ocasiones se ha tratado desde una perspectiva totalmente diferente, limitándola al derecho a la protección de datos, es el denominado derecho al olvido que trae causa de la conocida Sentencia del TJUE de 13 de mayo de 2014[270].

En la materia que nos ocupa y centrándonos en el estatus del motor de búsqueda: ¿trata datos o no? ¿Es responsable de ese tratamiento o no? Las posturas en este ámbito son muy variadas. Por un lado según Google Spain y Google Inc., la actividad de los motores de búsqueda no puede considerarse tratamiento de los datos que se muestran en las páginas web de terceros que presenta la lista de resultados de la búsqueda, dado que estos motores tratan la información accesible en Internet globalmente sin seleccionar entre datos personales y el resto de información. El demandante, los Gobiernos español, italiano, austriaco y polaco y la Comisión Europea sostienen que dicha actividad implica claramente un «tratamiento de datos», en el sentido de la Directiva 95/46, que es distinto del tratamiento de datos realizado por los editores de los sitios de Internet y persigue objetivos distintos al de éste. A su juicio, el gestor de un motor de búsqueda es «responsable» del tratamiento de datos efectuado por él, en el sentido que otorga la normativa de protección de datos, y ello desde el momento en que es él quien determina la finalidad y los medios de dicho tratamiento. Es el gobierno griego sin embargo el que mantiene una postura quizá más acorde con la filosofía general respecto a la posición de los PSI. Sostiene que la actividad

[270] Unión Europea. Tribunal de Justicia de la Unión Europea (Gran Sala). Caso Mario Costeja vs. Google. Sentencia de 13 de mayo de 2014. Acceso al texto de la Sentencia en el siguiente enlace: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

controvertida constituye tal «tratamiento», pero, en la medida en que los motores de búsqueda sirven de simples intermediarios, las empresas que los gestionan no pueden considerarse «responsables», salvo en los casos en los que almacenan datos en una «memoria intermedia» o una «memoria oculta» por un período de tiempo que supere lo técnicamente necesario. Es precisamente esta postura la que sostiene también el Abogado General que refleja la idea que desde aquí defendemos. Parte de recordar que el papel y la posición jurídica de los proveedores de servicios de motores de búsqueda en Internet –a diferencia de la normativa española- no está regulado expresamente en la normativa de la Unión; y en concreto subraya que los proveedores de servicios de motores de búsqueda en Internet, como Google, que no prestan su servicio como contrapartida de una remuneración por parte de los usuarios de Internet, parecen, por su condición, estar excluidos del ámbito de aplicación de la Directiva 2000/31, sobre el comercio electrónico. Sin embargo, y esto es lo relevante, el propio Abogado general señala muy acertadamente que, a pesar de ello, es necesario analizar su posición frente a los principios jurídicos que subyacen a las limitaciones de la responsabilidad de los proveedores de servicios de Internet. En otras palabras, saber en qué medida son actividades desarrolladas por un proveedor de servicios de motor de búsqueda en Internet, desde el punto de vista de los principios de responsabilidad, análogas a los servicios enumerados en la Directiva 2000/31, sobre el comercio electrónico, y en qué medida un proveedor de servicios de motor de búsqueda en Internet actúa como proveedor de contenidos por derecho propio. De hecho en su argumentario recurre a dicha filosofía subyacente y en concreto recuerda el considerando 47 de la Directiva, cuando afirma que el responsable del tratamiento de mensajes con datos personales transmitidos a través de un servicio de telecomunicaciones o de correo electrónico cuyo único objetivo sea transmitir mensajes de ese tipo, es la persona de quien procede el mensaje, y no la que ofrece el servicio de transmisión. Este considerando, así como las exenciones de responsabilidad establecidas en la Directiva 2000/31, sobre comercio electrónico (artículos 12, 13 y 14), se basa en el principio jurídico según el cual las relaciones automáticas, técnicas y pasivas con contenido almacenado o transmitido electrónicamente no generan ni control de éste ni responsabilidad sobre él. Añade en línea a esta exención de responsabilidad argumentos sostenidos por el propio Grupo de Trabajo del artículo 29. Según las autoridades de protección de datos europeas, el principio de proporcionalidad requiere que, en la medida en que un proveedor de un motor de búsqueda actúe exclusivamente como intermediario, no debe considerarse como responsable principal del tratamiento de datos personales

efectuado. En este caso, los responsables principales del tratamiento de datos personales son los proveedores de información.

Sin embargo, y como es conocido, la posición del PSI en este caso va mucho más allá en cuanto a la asunción de responsabilidad a juicio del TJUE. Afirma este que 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. Yen la cuestión que nos ocupa, es decir más allá de si trata o no de datos personales, considera que sí es un verdadero responsable. Para ello afirma 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. Y para justificarlo afirma que el tratamiento de datos personales llevado a cabo por un motor de búsqueda se distingue del efectuado por los editores de sitios de Internet, que consiste en hacer figurar esos datos en una página en Internet, y se añade a él. Esa añadidura que justifica otorgarle la condición de responsable se basa en gran medida en un doble argumento: por un lado la proyección exponencial que permite un motor de búsqueda, ya que señala el tribunal que actividad de los motores de búsqueda desempeña un papel decisivo en la difusión global de dichos datos en la medida en que facilita su acceso a todo internauta que lleva a cabo una búsqueda a partir del nombre del interesado, incluidos los internautas que, de no ser así, no habrían encontrado la página web en la que se publican estos mismos datos. Y por otro lado en las consecuencias que se pueden derivar para el usuario afectado, por cuanto afirma el tribunal que la organización y la agregación de la información publicada en Internet efectuada por los motores de búsqueda para facilitar a sus usuarios el acceso a ella puede conducir, cuando la búsqueda de los usuarios se lleva a cabo a partir del nombre de una persona física, a que éstos obtengan mediante la lista de resultados una visión estructurada de la

información relativa a esta persona que puede hallarse en Internet que les permita establecer un perfil más o menos detallado del interesado.

Pero al margen de esta disquisición respecto al estatus, que lógicamente tiene relevancia en cuanto a las consecuencias que la normativa de protección de datos otorga al responsable del tratamiento, la misma filosofía subyace respecto a quién debe dirigirse el afectado. Así, Google Spain y Google Inc. consideran que, en virtud del principio de proporcionalidad, cualquier solicitud que tenga por objeto que se elimine información debe dirigirse al editor del sitio de Internet de que se trate, ya que éste es quien asume la responsabilidad de publicar la información, quien puede examinar la licitud de esta publicación, y quien dispone de los medios más eficaces y menos restrictivos para hacer que esa información sea inaccesible. Además, consideran que imponer al gestor de un motor de búsqueda que retire de sus índices información publicada por los editores de sitios de Internet, no tiene en cuenta los derechos fundamentales del resto de los internautas y del propio gestor. Por su parte, el demandante, los Gobiernos español, italiano y polaco y la Comisión consideran que la autoridad nacional puede ordenar directamente al gestor de un motor de búsqueda que retire de sus índices y de su memoria intermedia información que contiene datos personales publicada por terceros, sin dirigirse previa o simultáneamente al editor de la página web en la que se ubica dicha información. Si bien es cierto que mientras a juicio del demandante, de los Gobiernos español e italiano y de la Comisión, el que dicha información se publicara de forma lícita y que siga figurando en la página web de origen carece de relevancia sobre las obligaciones de dicho gestor con arreglo a la Directiva 95/46; sin embargo, para el Gobierno polaco, este hecho le libera de sus obligaciones. En fin, la Sentencia señaló que los derechos a la intimidad y a la protección de datos prevalecen, no solo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público…tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el mencionado interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate.

El derecho al olvido ha supuesto sin duda una convulsión en el tratamiento de datos y en la posición de los buscadores. La existencia de un derecho absoluto se ha visto matizada y la posición de los buscadores y su grado de responsabilidad también. De nuevo recurrir al caso por caso a través de la jurisprudencia, pone de manifiesto la existencia de considerables matices. Para ello baste por ejemplo observar la STS de 29 de diciembre de 2014 se

planteaba el caso por el que AEPD consideraba que los buscadores en el ejercicio de su actividad, efectúan un tratamiento de datos de carácter personal por lo que están obligados a hacer efectivo el derecho de cancelación y/oposición del interesado que se opone a que se indexe y sea puesta a disposición de los internautas determinada información a él referente que se encuentra en páginas de tercero y permiten relacionarles con la misma. Además, señalaba también la AEPD, y esto es más relevante, que como intermediarios de la sociedad de información, según la Ley 34/2002, de Servicios de la Información y de correo electrónico (LSSI), los buscadores están sometidos a la normativa de protección de datos, estando obligados a atender los requerimientos que al amparo de los artículos 8 y 17 de la LSSI les dirija el Director de la AEPD para la adecuación del tratamiento de los datos a las disposiciones de la LOPD. Frente a dicha postura, el Tribunal Supremo introdujo matices y ello como consecuencia de que la resolución de la AEPD frente a la que se recurría, y la solicitud de cancelación de datos que dio origen a la misma, se referían a determinadas informaciones y datos personales del denunciante que no aparecían en una página Web (como había sido lo habitual en la mayoría de sentencias dictadas por el propio Tribunal con ocasión de la STJUE de 13 de Mayo de 2014) sino que figuraban en un blog, que no es sino un servicio prestado también por la propia recurrente por el que el titular o editor del blog incorpora determinada información, comentarios o datos que se alojan en una plataforma denominada blogger gestionada también por Google Spain, S.L. Hay que partir de que la resolución de la AEPD impugnada no se limitaba a acordar que Google Spain evitara la indexación de los datos personales del denunciante objeto de este procedimiento y que aparecen en el blog (lo que conecta con la actividad de Google Spain, S.L. como motor de búsqueda), sino que, además, acordaba la eliminación de dichos datos personales del blog alojado en la plataforma on line Blogger, que es un servicio de naturaleza distinta del buscador, si bien la titularidad de ambos es de la misma entidad nominada blogger gestionada también por Google Spain, S.L. Es por este importante matiz, que el Tribunal Supremo recuerda que en los casos en que la información o los datos cuya cancelación se solicita, se encuentran alojados en un blog, Google Spain, S.L. desempeña simultáneamente dos funciones: buscador y alojador de contenidos, ofreciendo al titular del blog la posibilidad de divulgar los contenidos que ha decidido incorporar a su blog. La obligación de retirada de los contenidos que sostiene la resolución de la AEPD deriva de esta segunda función de Google como simple plataforma o alojador de contenidos. Pues bien, con base en este hecho, el Tribunal recuerda que la plataforma Blogger en la que se encuentra alojado el blog que contiene los datos personales del denunciante al que se accede a través de la dirección

Web por él facilitada, no se cuestiona que se trata de un servicio de intermediación de la sociedad de la información, al igual que los buscadores. En este sentido la Ley 34/2002, de 11 de julio, incluye (Anexo b) como "servicio de intermediación", entre otros, el alojamiento en los propios servidores de datos. Ley que en sus artículos 8 y 16 limita la responsabilidad de los prestadores de dichos servicios de alojamiento o almacenamiento de datos respecto de la información almacenada a petición del destinatario, pero permite que se les pueda requerir para que retiren los datos que atenten a determinados principios (entre ellos la dignidad de la persona). Esta posibilidad de retirar contenidos también se recoge en la Política de Privacidad de la plataforma Blogger a la que se refiere la parte recurrente en su escrito de demanda. Por todo ello, como primera conclusión, el Tribunal afirma que el buscador no es responsable de los contenidos del blog sino que es una plataforma, un alojador de contenidos, un intermediario entre el editor del Blog y los usuarios, por lo que se plantea hasta qué punto será posible imponerle la obligación que recoge la parte dispositiva de la resolución de la AEPD de eliminar el contenido en el marco de un procedimiento de tutela de derechos, contemplado en la LOPD. Y en respuesta niega la responsabilidad subrayando por un lado, como error de procedimiento, que la AEPD ha tramitado el expediente sin realizar el trámite de audiencia y por otro, en lo que nos interesa, que no ha quedado acreditado que Google sea el responsable del fichero que integra el blog en el que está la información y los datos a los que se refiere el denunciante.

3.2.2.4.5 Una sucinta visión comparada más allá de las fronteras europeas: Estados Unidos, Argentina y Australia.

La realidad es que esta materia y estos debates a los que nos conduce la responsabilidad de los PSI no son exclusivos, como resulta lógico, del continente europeo, aunque llama la atención que la legislación sí que se utiliza en muchas ocasiones como argumento de fuerza. A título de ejemplo, en Argentina tuvo mucha repercusión la Sentencia de su Corte Suprema de 28 de octubre de 2014 en el caso Rodríguez contra Google[271] en el que sentó como criterio, en línea muy aproximada a la evolución de la jurisprudencia de nuestro tribunal supremo, que es necesario el conocimiento efectivo para atribuir responsabilidad subjetiva al prestador de servicios de intermediación, y añade que basta una notificación privada en aquellos casos en que el daño resulte manifiesto y grosero, mientras que es necesaria la

[271] Argentina. Corte Suprema. Caso Rodríguez vs. Google Inc. Sentencia de 28 de octubre de 2014. Acceso al texto de la Sentencia en el siguiente enlace: http://www.telam.com.ar/advf/documentos/2014/10/544fd356a1da8.pdf

notificación administrativa o judicial en los casos en que es opinable, dudoso o exige un esclarecimiento,. Esta doctrina fue posteriormente ratificada en una sentencia similar de 30 de diciembre de 2014[272].

En Estados Unidos el debate de esta cuestión se remonta incluso hasta 1995. Se trata de la Sentencia del Tribunal de Distrito Norte de California [273] en la que se dirimía la responsabilidad que tenían que asumir tanto un servicio de anuncios local (*Bulletin Board Service, BBS)* como, en lo que nos interesa, el proveedor de acceso a Internet, Netcom, y ello como consecuencia de que a través de un servidor de noticas controlado por Netcom, se subieron archivos que contenían material de la Iglesia de la Cienciología protegido por los derechos de autor. El tribunal señaló que ninguno de los dos era responsable de haber infringido derechos de autor por cuanto ninguno había llevado a cabo actuaciones destinadas a realizar las copias. Aunque los sistemas informáticos de ambas partes operaban automáticamente para recibir y transmitir los contenidos de los suscriptores, el tribunal consideró que ello no era suficiente para hablar de una responsabilidad directa. En cuanto a la responsabilidad indirecta, el tribunal también se pronunció contra la referida iglesia señalando que no había una recompensa económica directa para los dos prestadores derivada de dichas publicaciones. Sin embargo sí que afirmó el tribunal que el proveedor de acceso a Internet podría ser responsable bajo la teoría de la contribución al daño por haber contribuido materialmente a la infracción del usuario. Sin embargo, el tribunal reconoció que podría no haber responsabilidad incluso bajo esta perspectiva salvo que Netcom conociera de la infracción. Subrayó que si hubiera conocido o hubiera tenido que conocer de la presencia de materiales protegidos por derechos de autor en su servidor y no los hubiera retirado, podría haber contribuido a la infracción y consiguientemente se hubiera derivado la responsabilidad. Precisamente la teoría de la contribución al daño ha sido utilizada por la doctrina norteamericana en numerosas ocasiones y está basada en la ausencia de pasividad y neutralidad por parte de los PSI. En el marco de la jurisprudencia norteamericana, mayor impacto incluso que el ámbito de los derechos de autor, ha tenido la difamación, como concepto comprensivo de las injurias y las calumnias. Existen al respecto dos casos

[272] Argentina. Corte Suprema. Caso Da Cunha, Virginia c/ Yahoo de Argentina. Sentencia de 30 de diciembre de 2014. Acceso al texto de la Sentencia en el siguiente enlace: http://www.saij.gob.ar/csjn-ratifica-buscadores-internet-carecen-responsabilidad-objetiva-contenidos-publicados-nv10123-2014-12-30/123456789-0abc-321-01ti-lpssedadevon

[273] Estados Unidos. Tribunal de Distrito Norte de California. Caso Religious Technology Center v. Netcom On-Line Communication Services, Inc.Sentencia de 21 de noviembre de 1995, Acceso al texto completo de la sentencia en el siguiente enlace: https://www.law.cornell.edu/copyright/cases/907_FSupp_1361.htm

emblemáticos cuales son el caso *Stratton Oakmont, Inc. v. Prodigy Services Co* que dictó el Tribunal Supremo de Nueva York en 1995[274], y el caso *Cubby, Inc. v. CompuServe Inc* dictado por el Tribunal del Distrito Sur de Nueva York en 1991[275]. En el primer supuesto se demandó a la empresa Prodigy por difamación debido a los comentarios vertidos por uno de sus clientes en un foro de debate. La cuestión clave en la que entró el tribunal fue en determinar si Prodigy era un distribuidor de información como una librería o una biblioteca, o si se trataba de un editor de información, como en el caso de un periódico. En el primer caso no sería responsable, sin embargo en el segundo supuesto sí sería responsable. En la decisión el juez señaló que debido a las políticas de vigilancia y censura de sus foros, que estaban claramente publicitadas, Prodigy era un editor y consiguientemente era potencialmente responsable por los contenidos difamatorios. Al final el caso concluyó por un acuerdo entre las partes. Resulta sin duda paradójico que el establecimiento de unas normas de uso derive en la asunción de un régimen de responsabilidad más estricto. Prueba de esta paradoja es que en el caso de Compuserve los hechos eran muy similares, pero sin embargo el tribunal consideró que nos encontrábamos ante un simple distribuidor de información y consiguientemente no responsable. Es decir, no fue responsable debido al desconocimiento de las declaraciones y porque no había ninguna razón para que las pudiera conocer.

En fin, en otras latitudes también se ha planteado este debate. Es el caso de la Sentencia del Tribunal Supremo del Sur de Australia de 27 de octubre de 2015[276] en el caso *Duffy vs. Google*. Se trataba de un supuesto en el que la demandante, la Dra. Duffy, había consultado a una serie de médiums online a través de una web denominada Kasamba. Posteriormente había realizado varios comentarios e informes en una página web y había creado un chat con quejas respecto a algunos de los médiums consultados. Posteriormente un número de informes y comentarios se recogieron en la referida página web haciendo alegaciones contra la citada doctora quien, cuando tuvo conocimiento de que las búsquedas en google a través de su nombre derivaban en dichos materiales lo notificó a Google y le pidió que retirara ese

[274] Estados Unidos. Tribunal Supremo de Nueva York. Caso Stratton Oakmont, Inc. v. Prodigy Services Co. Sentencia de 3 de octubre de 1995. Acceso al texto de la Sentencia en el siguiente enlace: https://w2.eff.org/legal/cases/Stratton_Oakmont_Porush_v_Prodigy/stratton-oakmont_porush_v_prodigy_et-al.decision

[275] Estados Unidos. Tribunal del Distrito Sur de Nueva York. Cubby, Inc. vs. CompuServe Inc, Sentencia de 29 de octubre de 1991. Acceso al texto de la Sentencia en el siguiente enlace: https://epic.org/free_speech/cubby_v_compuserve.html

[276] Australia. Tribunal Supremo del Sur de Australia. Caso Duffy vs. Google. Sentencia de 27 de octubre de 2015. Acceso al texto completo de la Sentencia en el siguiente enlace: http://www.austlii.edu.au/au/cases/sa/SASC/2015/170.html

contenido difamatorio que lo era además de manera manifiesta. Además se incorporó a la demanda también la herramienta de google de autocompletar que se concretaba en "*Janice duffy psychic stalker*" (Janice Duffy acosadora de médiums). Se dictó Sentencia declarando la responsabilidad de Google por el contenido injurioso de los hipervínculos y los fragmentos que mostraba el buscador cuando se introducía el nombre de la demandante y por el contenido injurioso de las búsquedas derivadas de la función autocompletar en lo referido a su nombre. Además, de manera más controvertida, google fue considerado responsable en cuanto que reeditor del contenido de páginas web de terceros enlazadas en sus resultados de búsqueda. Los motivos para sostener la responsabilidad de Google por parte del tribunal fueron fundamentalmente tres: primero que Google había publicado los resultados de búsqueda sobre el nombre de la doctora en forma de título, fragmento, URL que contenían texto de y enlaces a 16 páginas externas cuyos resultados eran por sí mismos difamatorios; en segundo lugar que por razón de la publicación de dicho texto y enlaces al material del Informe Ripoff en sus resultados de búsqueda, Google era un reeditor de dicho material en las páginas web externas; y en tercer lugar que Google publicaba las palabras "*janice duffy psychic stalker*" a través de su función Autocompletar.

En definitiva la casuística expuesta pone de manifiesto que estamos ante uno de los temas que generan una mayor controversia, aunque parece haber unas líneas relativamente claras de actuación; a la par que se trata de una cuestión de gran un impacto directo respecto de la existencia o no de límites a la libertad de expresión en Internet. El elemento colaborativo de la información en la web, su estructura de extremo a extremo hace que todos podamos ser creadores y receptores de contenidos y consiguientemente la fijación de quién puede limitar dichos contenidos es, y seguirá siendo, uno de los grandes debates.

3.3 El derecho a la protección de datos como derecho de cuarta generación.

3.3.1 El derecho a la protección de datos en el continente europeo.

Para terminar con este capítulo introductorio debemos adentrarnos en uno de los derechos de cuarta generación por excelencia –puesto que surge en el contexto de la sociedad de la información– y que va a constituir el punto de partida de nuestro análisis: el derecho a la protección de datos. Conocer su evolución histórica, su plasmación normativa y sus grandes principios, servirá como punto de partida para el posterior análisis de en qué medida este

derecho fundamental –con su actual tratamiento jurídico– está salvaguardado en el entorno de la computación en nube.

Más allá de la delimitación conceptual, que necesariamente se ha llevado a cabo más arriba para diferenciarlo del derecho a la intimidad, desde un punto de vista histórico el derecho a la protección de datos tiene sus primeras manifestaciones jurídicas en los Estados Unidos y en Europa en la década de los setenta a través de normas como la Ley del Land de Hesse de 1970 que regulaba las bases de datos de la Administración, la Ley sueca de 11 de mayo de 1973 sobre protección de datos, la ley de Renania Palatinado en 1974 o la *Fair Credit Reporting Act*, de 26 de octubre de 1970, en Estados Unidos[277]. Precisamente en la segunda mitad de los setenta se dictaron leyes también en otros países europeos como Dinamarca, Francia, Alemania, Luxemburgo y Noruega.

Sin embargo previamente, en el seno del Consejo de Europa, ya se había dado alguna iniciativa de naturaleza política, así a través de la Resolución 509 de su Asamblea parlamentaria en 1968 sobre "Los derechos humanos y los nuevos logros científicos y técnicos"[278], así como en las Resoluciones del Comité de Ministros de 1973 sobre protección de la privacidad de los individuos frente a los bancos de datos electrónicos en el sector privado[279], y de 1974 sobre protección de la privacidad de los individuos vis a vis los bancos de datos electrónicos en el sector público[280].

Su constitucionalización, como hemos visto, se dio en la Constitución portuguesa de 1976 y en la española de 1978[281], y también con un instrumento legal diferente en el caso de Austria,

---

[277] LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa*. Temas Clave de la Constitución española, Tecnos, 1990. 207 p FERNÁNDEZ SEGADO, F., La dinamización de los mecanismos de garantía de los derechos y de los intereses difusos en el Estado social, ob. Cit.

[278] CONSEJO DE EUROPA. Asamblea parlamentaria. Resolución 509 de 31 de enero de 1968 sobre Los derechos humanos y los nuevos logros científicos y técnicos. Disponible en web: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=14546&lang=en

[279] CONSEJO DE EUROPA. Comité de Ministros. Resolución 22 de 26 de septiembre de 1973 sobre protección de la privacidad de los individuos vis a vis los bancos de datos electrónicos en el sector privado. Disponible en web: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680502830

[280] CONSEJO DE EUROPA. Comité de Ministros. Resolución 29 de 20 de septiembre de 1974 sobre protección de la privacidad de los individuos vis a vis los bancos de datos electrónicos en el sector público. Disponible en web: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d1c51

[281] Hay que mencionar que, aunque está generalizada la consideración de que el derecho a la autodeterminación informativa, la libertad informática o el derecho a la protección de datos se fundamentan en el art. 18.4 de la Constitución, no es sin embargo una postura unánime. En su voto particular a la Sentencia del Tribunal Constitucional 290/2000, el Magistrado Jiménez de Parga afirmaba por ejemplo que

país en el que el artículo 1 de la Ley de Protección de Datos de 1978 lo declaraba como derecho fundamental; pasándose luego a su reconocimiento internacional a través del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981 y a su plasmación jurisprudencial en la Sentencia del Tribunal Constitucional Federal alemán sobre la ley del censo de 1983 en la que se señaló que tan importante era reconocer unas esferas personales dignas de protección y reservadas frente al conocimiento ajeno, como reconocer las facultades de control de tales zonas y de los datos que se generaran en ellas (*Recht auf informationalle Selbsbestimmung*)[282]. Esta Sentencia añadía que de otro modo se dañaría no solo las oportunidades personales para el desarrollo personal sino también el bien común, porque la autodeterminación es una condición básica de una comunidad democrática libre que está basada en la posibilidad de sus ciudadanos para actuar y para colaborar[283].

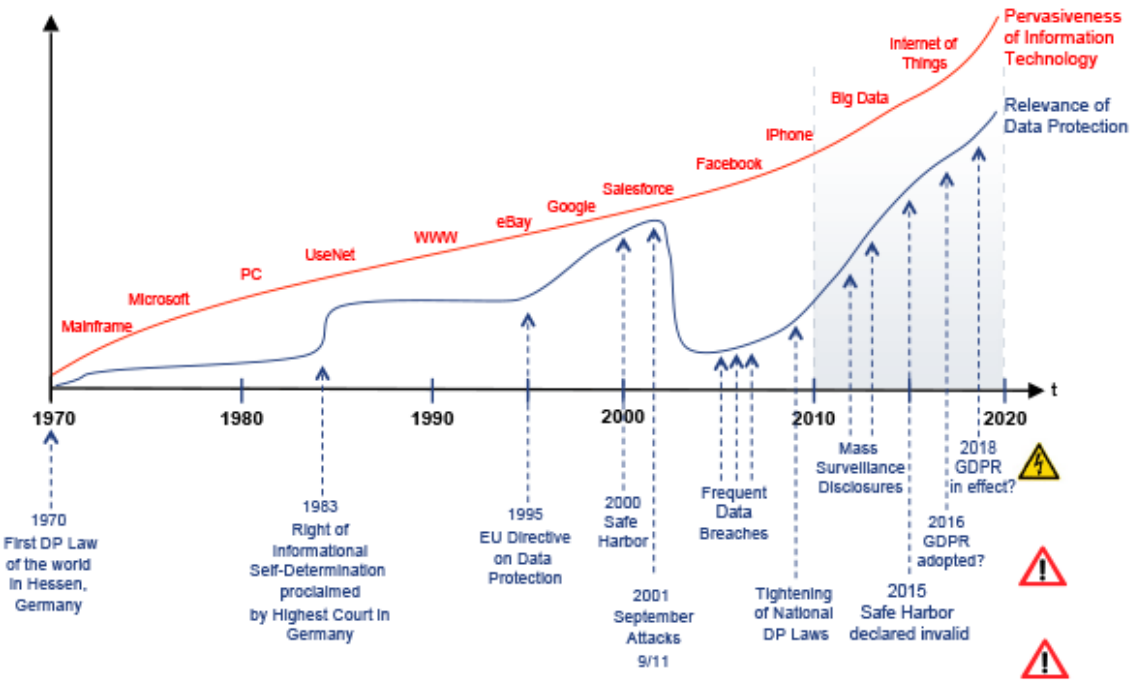
Estas manifestaciones hacen que no podamos compartir la postura de Canales Gil respecto a que hasta la década de los noventa no se puede hablar de un reconocimiento del derecho a la protección de datos como un derecho fundamental[284]. Cierto es sin embargo que el desarrollo legislativo propiamente dicho, no llegó hasta esos años, pero ello no es motivo para dicha afirmación, salvo que se tenga una visión positivista a ultranza de los derechos fundamentales que desde estas líneas no compartimos.

el derecho a la autodeterminación informativa no se encuentra expresamente en la Constitución y defendía su fundamentación partiendo del artículo 10.1 de la Constitución y su configuración con base en los arts. 18.1 y 20.1.

[282] Síntesis de la Sentencia tomada de MEGÍA QUIRÓS, J.J., ob. cit., p. 538.

[283] Tomado de PETERSEN, T. y ESCHE, A., Perserving an Old Model in the New World: German Economic Policy [en línea], *Newpolitik,* octubre 2016. Disponible en web: http://www.bfna.org/sites/default/files/publications/Echoes_of_history_Understanding_German_Data_Protection_Freude.pdf

[284] CANALES GIL, A., ob. cit. , pp. 19 y 20.



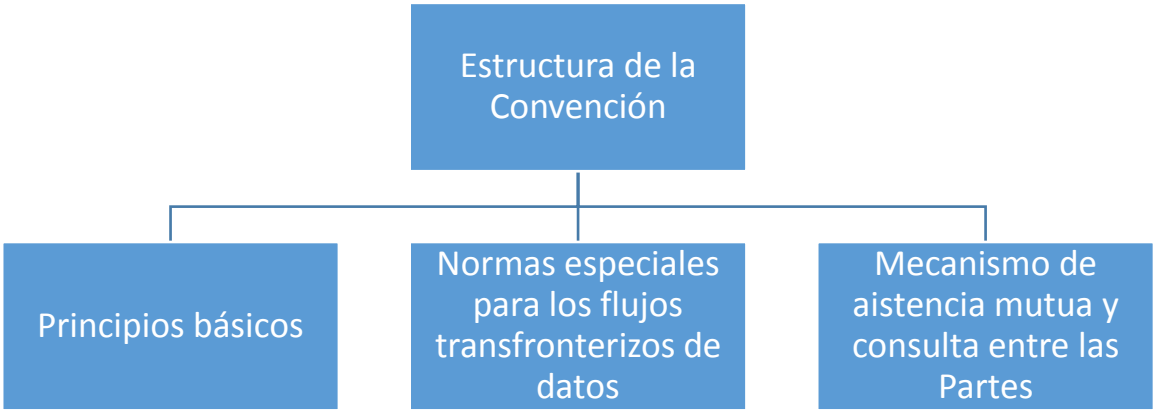
Fuente: Ernst-Oliver Wilhelm. A brief history of the General Data Protection Regulation[285]

Dentro de los textos citados, resulta obligado detenerse en la Convención 108 del Consejo de Europa porque suponía la primera vez que en un texto normativo marca los principios esenciales en torno a los cuales va a girar la regulación de la protección de datos. Estamos efectivamente ante una construcción principialista que impregna de manera inevitable cualquier acercamiento a la regulación de los impactos de la tecnología en la vida social. Sin entrar en mayores disquisiciones, la velocidad a la que evoluciona la tecnología hace que sea imprescindible una cierta inteligencia normativa y dejar el detalle a los supuestos que sean absolutamente inevitables. Lo dijo ya hace muchos años el maestro García de Enterría cuyas palabras reproducimos: "La superioridad del Derecho Romano sobre otros sistemas jurídicos históricos anteriores o posteriores estuvo justamente, no ya en la mayor perfección de sus leyes, sino en que sus juristas fueron los primeros que se adentraron en una jurisprudencia según principios, la cual ha acreditado su fecundidad, e incluso, paradójicamente, su perennidad, y hasta su superior certeza, frente a cualquier código perfecto y cerrado de todos los que la historia nos presenta"[286]. Volviendo a lo concreto, el

[285] WILHELM, E.O., *A brief history of the General Data Protection Regulation*. Disponible en web: https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/

[286] GARCÍA DE ENTERRÍA, E., Reflexiones sobre la Ley y los Principios Generales del Derecho, *Revista de Administración Pública,* Enero-abril 1963, nº 40, p. 189-222.

referido texto contempla, entre otros, el principio de calidad de los datos, verdadero pilar como veremos de este nuevo derecho fundamental; la categorización de los mismos; la referencia a la seguridad; o los flujos transfronterizos. Todos ellos son conceptos que no resultan novedosos, pero que en dicho momento sin duda se podían catalogar de revolucionarios.

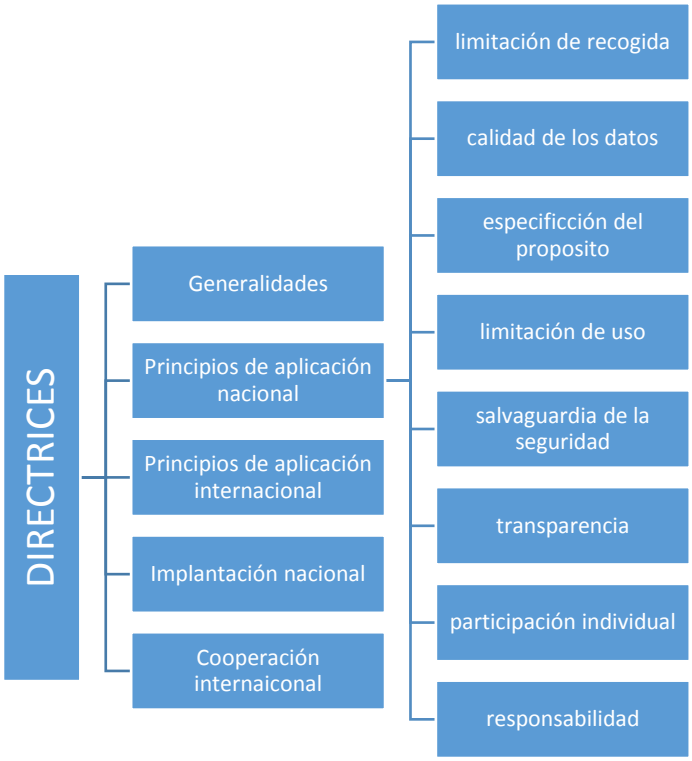


Fuente: elaboración propia

Esta Convención se vio completada en el año 2001 cuando se adoptó un Protocolo Adicional introduciendo una serie de previsiones sobre la transferencia de datos a países no miembros (países terceros) y sobre el establecimiento vinculante de autoridades nacionales de protección de datos. Otro factor a tener en cuenta a la hora de subrayar su importancia es que es un texto abierto a Estados no miembros del Consejo de Europa y consiguientemente se puede acabar convirtiendo en un estándar internacional de enorme utilidad por su carácter vinculante. En el momento de escribir estas líneas, dicha Convención se encuentra ya en vigor en Uruguay, Mauricio y Senegal; mientras que el proceso se encuentra abierto en Cabo Verde, Marruecos y Túnez.

También en el ámbito internacional y prácticamente en paralelo a la referida Convención del Consejo de Europa, la OCDE aprobó el 23 de septiembre de 1980 unas Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales que, como señala la propia organización y en línea con lo que hemos apuntado, contempla una serie de principios que “se caracterizan por su claridad y flexibilidad de aplicación, y por su formulación, que es lo suficientemente general para permitir su adaptación a los cambios tecnológicos”. Las

citadas Directrices tienen la estructura descrita en la siguiente figura, donde cabe destacar en particular los principios de aplicación nacional que, en línea con los ya apuntados, son los que inspiran la normativa de protección de datos desde sus orígenes:



Fuente: elaboración propia

La jurisprudencia del TEDH ha tenido ya oportunidades para pronunciarse en numerosas ocasiones sobre la protección de datos, a pesar de que, como recordamos, no está expresamente recogido como tal derecho fundamental en la CEDH. Cabe recordar al respecto la conocida STEDH de 1978 en el caso *Tyrer vs. the United Kingdom*[287] en la que el Tribunal recordaba que "la Convención es un instrumento vivo que, como ha resaltado correctamente el Comité, debe ser interpretado a la luz de las condiciones actuales". Sí cabe decir que no fue hasta los años noventa cuando empezó un reconocimiento expreso de ese derecho en la jurisprudencia del TEDH, así en la STEDH en el caso *Z vs. Finland*[288], caso en

[287] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Plenario). Caso Tyrer vs. Reino Unido. Sentencia de 25 de abril de 1978. Acceso al texto de la Sentencia en el siguiente enlace: http://hudoc.echr.coe.int/eng#{"fulltext":["Tyrer"],"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-57587"]}

[288] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Plenario). Caso Z vs. Finlandia. Sentencia de 25 de febrero de 1997. Acceso al texto de la Sentencia en el siguiente enlace:

el que se había procedido a la revelación de que una persona tenía el SIDA en un procedimiento criminal contra su marido. El TEDH consideró que se había producido una violación del artículo 8 de la Convención, considerando que la revelación de dicho dato a la prensa no estaba amparada en ninguna razón convincente y que la publicación de la información había dado lugar a una violación de su derecho a la vida privada. El TEDH señaló en particular que el respeto a los datos médicos es un principio vital en los sistemas jurídicos de los Estados miembros de la Convención y que es crucial no solamente el respeto a la privacidad del paciente sino también la preservación de su confianza en la profesión médica y en los servicios sanitarios en general. Efectivamente, reiteramos, la ausencia de una mención expresa en la CEDH al derecho a la protección de datos ha hecho que siempre se haya recurrido al concepto de vida privada previsto en el artículo 8. A este respecto, la STEDH del caso *Marper vs. Reino Unido*[289] señaló que el mero almacenamiento de datos referidos a la vida privada de una persona equivale a una interferencia en el sentido del artículo 8, y añadía que el posterior uso de dicha información no afecta a dicha conclusión; al igual que la STEDH en el caso *LH vs. Letonia*[290] en la que de nuevo se recordaba la importancia de proteger los datos médicos para que una persona disfrute del derecho a que se respete su vida privada.

Partiendo de dicho reconocimiento, el TEDH ya se ha pronunciado en infinidad de ocasiones sobre el derecho a la protección de datos y distintos aspectos vinculados al mismo[291], como por ejemplo respecto al tipo de datos que quedarían amparados. Se han incluido la identidad de género el nombre, la orientación sexual o la vida sexual en el caso *Bensaid vs United*

http://hudoc.echr.coe.int/eng#{"languageisocode":["ENG"],"appno":["22009/93"],"documentcollectionid2":["CLIN"],"itemid":["002-9432"]}

[289] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Gran Sala). Caso Marper vs. Reino Unido. Sentencia de 4 de diciembre de 2008. Acceso al texto de la Sentencia en el siguiente enlace: http://hudoc.echr.coe.int/eng#{"itemid":["001-90051"]}

[290] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Sección Cuarta). Caso LH vs Letonia. Sentencia de 29 de abril de 2014. Acceso al texto de la Sentencia en el siguiente enlace: http://hudoc.echr.coe.int/eng#{"fulltext":["LH LATVIA"],"sort":["kpdate Ascending"],"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-142673"]}

[291] La mayoría de las referencias tomadas de CONSEJO DE EUROPA. TRIBUNAL EUROPEO DE DERECHOS HUMANOS. AGENCIA EUROPEA DE DERECHOS FUNDAMENTALES. *Handbook on European data protection law*. 2014. Disponible en Web: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf. Igualmente hay referencias tomadas de RAMOS ROMEU, F., *Data Protection in the ECHR`s case law*, así como de CONSEJO DE EUROPA. European Court of Human Rights. Factsheet – Personal data protection. November 2016. Disponible en web: http://www.echr.coe.int/Documents/FS_Data_ENG.pdf

Kingdom[292], donde se procedió a la expulsión del país de una persona esquizofrénica; la raza, el nombre o los datos para establecer vínculos familiares en el caso *Burghartz vs Switzerland*[293] donde se negaba a un matrimonio la posibilidad de utilizar el apellido de la mujer, por el que habían optado cuando se casaron en Alemania, como nombre de familia; la propia imagen en el caso *Sciacca vs Italy*[294], en el que se repartió la fotografía de una persona que no tenía relevancia pública en una rueda de prensa por parte del fiscal y sin ninguna finalidad investigadora; las imágenes en el caso *Peck vs United Kingdom*[295] donde se facilitó a los medios las imágenes grabadas en una calle por un circuito cerrado de televisión instalado por el ayuntamiento y en las que se mostraba a una persona cortándose las muñecas; la voz en el caso *P.G. and J.H. vs. the United Kingdom*[296], donde se grabó la voz de una persona en una comisaría de policía sin su consentimiento; el ADN en el caso *Peruzzo and Martens vs. Germany*[297] donde se recurrió respecto a la orden de los tribunales nacionales de almacenar material celular de los recurrentes, que habían sido condenados previamente, en una base de datos en forma de perfiles de ADN con la finalidad de facilitar la investigación de potenciales futuros crímenes; los datos de localización en el caso *Uzun vs. Germany*[298], donde el recurrente, sospechoso de estar envuelto en unos ataques con bomba a cargo de un movimiento radical de izquierdas, recurrió respecto al sistema de vigilancia vía GPS y al uso de los datos obtenidos en un procedimiento penal contra él; las huellas dactilares en el caso *M.K. vs. France*[299] donde el TEDH consideró como vulnerador

---

[292] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Sección tercera). Caso Bensaid vs. Reino Unido. Sentencia de 6 de febrero de 2001. Acceso al texto de la Sentencia en el siguiente enlace: http://www.bailii.org/eu/cases/ECHR/2001/82.html

[293] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Pleno). Caso Burghartz vs Suiza. Sentencia de 22 de febrero de 1994. Acceso al texto de la Sentencia en el siguiente enlace: http://www.lawschool.cornell.edu/womenandjustice/upload/Burghartz.PDF

[294] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Sección cuarta). Caso Sciacca vs. Italia. Sentencia de 11 de enero de 2005. Acceso al texto de la Sentencia en el siguiente enlace: http://www.5rb.com/wp-content/uploads/2013/10/Sciacca-v-Italy-ECHR-11-Jan-2005.pdf

[295] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Sección cuarta). Caso Peck vs. Reino Unido. Sentencia de 28 de enero de 2003. Acceso al texto de la Sentencia en el siguiente enlace: http://portal.nasstar.com/75/files/Peck-v-UK%20ECHR%2028%20Jan%2003.pdf

[296] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Sección tercera). Caso P.G. y J.H vs. Reino Unido. Sentencia de 25 de septiembre de 2001. Acceso al texto de la Sentencia en el siguiente enlace: http://www.bailii.org/eu/cases/ECHR/2001/550.html

[297] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Sección quinta). Caso Peruzzo y Martens vs. Alemania. Sentencia de 4 de junio de 2013. Acceso al texto de la Sentencia en el siguiente enlace: http://hudoc.echr.coe.int/eng#{"display":[2],"languageisocode":["ENG"],"appno":["57900/12"],"itemid":["001-121998"]}

[298] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Sección quinta). Caso Uzun vs. Alemania. Sentencia de 2 de septiembre de 2010. Acceso al texto de la Sentencia en el siguiente enlace: http://hudoc.echr.coe.int/eng#{"fulltext":["UZUN V. GERMANY"],"itemid":["001-100293"]}

[299] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Sección quinta). Caso M.K. vs. Francia. Sentencia de 18 de julio de 2013. Acceso al texto de la Sentencia en el siguiente enlace: http://hudoc.echr.coe.int/fre#{"itemid":["001-119075"]}

del derecho a la vida privada el no borrado de una base de datos de las huellas dactilares de una persona que había resultado sospechosa pero no condenada; los mensajes en el caso *Taylor-Sabori vs. the United Kingdom*[300] donde se interceptaron los mensajes en el busca particular de una persona como parte de una operación encubierta de la policía; o los datos profesionales en el caso *Sõro vs. Estonia*[301] donde se publicó que el recurrente había sido empleado durante la época soviética como conductor del KGB en el Boletín Oficial Estonio.

Más allá de la amplitud del concepto de dato que ha sido recogido por la referida jurisprudencia, resulta igualmente relevante tener en cuenta que el TEDH se ha pronunciado sobre diferentes aspectos relativos al ciclo de vida de los datos así como con respecto a principios esenciales de su tratamiento jurídico. Así, en la STEDH del caso *M.M. vs. the United Kingdom*[302], destacaba todo el ciclo de vida de los datos. Se trataba de un caso en el que el recurrente, que vivía en Irlanda del Norte, fue arrestado por la policía después de desaparecer con su nieto, bebé en ese momento, durante un día, en un intento por evitar su partida a Australia debida a la ruptura del matrimonio de su hijo. Debido a las circunstancias en las que tuvo lugar el incidente, las autoridades decidieron no acusarle y a cambio fue amonestado por secuestro de niños. La amonestación en principio iba a permanecer en su historial durante cinco años, pero debido a un cambio en la política en los casos en que la parte afectada fuera un niño, dicho periodo se extendería de por vida. En 2006, el recurrente recibió una oferta de empleo como trabajador sanitario sujeto a investigación, pero la oferta se retiró cuando el potencial empleador observó los antecedentes penales. Al margen de que el TEDH dio la razón al recurrente, en lo que ahora nos importa y dentro de su argumentación recordó que “hay varios momentos cruciales en los que aspectos de la protección de datos bajo el artículo 8 de la Convención pueden surgir, incluyendo durante la recogida, almacenamiento, utilización y comunicación de los datos. En cada una de esas fases, debe estar vigente una salvaguarda apropiada y adecuada que refleje los principios elaborados en

[300] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Sección segunda). Caso Taylor-Sabori vs. Reino Unido. Sentencia de 22 de octubre de 2002. Acceso al texto de la Sentencia en el siguiente enlace: http://www.bailii.org/eu/cases/ECHR/2002/691.html

[301] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Sección primera). Caso Sõro vs. Estonia. Sentencia de 3 de septiembre de 2015. Acceso al texto de la Sentencia en el siguiente enlace: http://hudoc.echr.coe.int/eng#{"itemid":["001-156518"]}

[302] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Sección cuarta). Caso M.M. vs Reino Unido. Sentencia de 13 de noviembre de 2012. Acceso al texto de la Sentencia en el siguiente enlace: http://www.bailii.org/eu/cases/ECHR/2010/1588.html

los instrumentos de protección de los datos y prevenga una interferencia en el artículo 8 arbitraria y desproporcionada" (párrafo 99 de la Sentencia).

Este pronunciamiento general de todo el ciclo de vida ha tenido manifestaciones concretas en cada uno de los estadios. En lo referido a la recogida por ejemplo la STEDH en el caso *L.H. vs. Latvia*[303] consideró que se había vulnerado el derecho a la vida privada en un caso en el que se recogieron datos médicos de la recurrente por una agencia estatal sin su consentimiento; o, también en el momento de la recogida de los datos, la STEDH en el caso *Dragojević vs. Croatia*[304] concerniente a la vigilancia secreta de las comunicaciones telefónicas de un sospechoso de tráfico de drogas y en la que el TEDH consideró vulnerado el derecho a la vida privada porque el juez de instrucción había incumplido el procedimiento que la ley croata establece para acreditar que la vigilancia secreta era necesaria y justificada en el caso concreto. También el almacenamiento y uso de los datos se ha tratado en diversas ocasiones. En el caso *Shimovolos vs. Rusia* [305]en el que se procedió a registrar a activistas de derechos humanos en la base de datos de vigilancia, que recogía información sobre sus movimientos, por tren o aire, dentro de Rusia; y que el TEDH declaró vulnerador del derecho a la vida privada ya que la creación y el mantenimiento de dicha base de datos y el procedimiento para su operativa, se regían por una orden ministerial que nunca se había publicado y consiguientemente no era accesible al público. Respecto al uso inadecuado de los datos, en el caso *L.L. vs. Francia*[306], el TEDH consideró que se había vulnerado el derecho a la vida privada al utilizar los tribunales documentos del historial médico del recurrente en un procedimiento de divorcio sin su consentimiento y pudiendo haber llegado a las mismas conclusiones sin su utilización; o el caso *Vukota-Bojic vs. Switzerland*[307] en el que el recurrente tras haberse visto envuelto en un accidente de tráfico, reclamó una pensión

[303] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Sección cuarta). Caso L.H. vs. Letonia. Sentencia de 29 de abril de 2014. Acceso al texto de la Sentencia en el siguiente enlace: http://hudoc.echr.coe.int/eng#{"itemid":["001-142673"]}

[304] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Sección primera). Caso Dragojević vs. Croacia Sentencia de 15 de mayo de 2015. Acceso al texto de la Sentencia en el siguiente enlace: http://hudoc.echr.coe.int/eng#{"itemid":["001-150298"]}

[305] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Sección primera). Caso Shimovolos vs. Rusia. Sentencia de 21 de junio de 2011. Acceso al texto de la Sentencia en el siguiente enlace: http://www.refworld.org/docid/4e26e4d32.html

[306] Consejo de Europa. Tribunal Europeo de Derechos Humanos (sección segunda). Caso L.L vs. Francia. Sentencia de 10 de octubre de 2006. Acceso al texto de la Sentencia en el siguiente enlace:http://hudoc.echr.coe.int/eng#{"itemid":["001-77356"]}

[307] Consejo de Europa. Tribunal Europeo de Derechos Humanos (sección tercera). Caso Vukota-Bojic vs. Switzerland. Sentencia de 18 de octubre de 2016. Acceso al texto de la Sentencia en el siguiente enlace: http://hudoc.echr.coe.int/eng#{"itemid":["001-167490"]}

de discapacidad. En el pleito con su aseguradora, esta llegó a contratar investigadores privados para llevar a cabo una vigilancia y utilizaron las evidencias en el procedimiento judicial. El TEDH señaló que dicha vigilancia había supuesto una injerencia en su vida privada, a pesar de haberse llevado a cabo en lugares públicos, por cuanto los investigadores habían recogido y almacenado los datos de una manera sistemática y los habían utilizado para una finalidad concreta; a lo que añadió que la ley suiza en la que se habían basado no era suficientemente precisa. En la fase de revelación de los datos también se ha pronunciado el TEDH en el caso *Panteleyenko vs. Ucrania*[308], cuando un tribunal permitió el uso en una audiencia de información confidencial sobre la salud mental y el tratamiento psiquiátrico de una persona cuando no resultaban datos necesarios para el juicio en sí mismo. O en la misma línea el caso *Biriuk vs. Lithuania* [309] cuando el diario de mayor tirada de dicho país publicó un artículo sobre la amenaza del SIDA en una parte remota de Lituania y se incluía en que el personal médico de un centro de tratamiento y un hospital habían confirmado que el recurrente tenía dicha enfermedad y lo describían como "notoriamente promiscuo" y que tenía dos hijos ilegítimos. El TEDH señaló que era crucial que la ley nacional salvaguardara la confidencialidad y evitara cualquier revelación de datos personales, particularmente teniendo en cuenta el impacto negativo que dichas revelaciones tienen en la voluntad de otros para someterse a los test y buscar tratamientos adecuados. En cuanto al borrado y destrucción de los datos, en el caso *Rotaru vs. Rumania*[310], el TEDH señaló que la ley rumana era inadecuada, entre otros aspectos, en lo referido al no establecimiento de límites a la vida de la información o el tiempo durante el cual se puede mantener, máxime que en este caso se estaba hablando de la información de la que disponía el Servicio de Inteligencia Rumano (RIS) respecto a que una persona había sido condenada en 1948 a un año de prisión por haber criticado el comunismo. Por último cabe subrayar también el reconocimiento de los aspectos subjetivos del derecho a la protección de datos (algunos de los cuales como el borrado ya han quedado reflejados más arriba) como el específico del

[308] Consejo de Europa. Tribunal Europeo de Derechos Humanos (sección quinta) Caso Panteleyenko vs. Ucrania. Sentencia de 29 de junio de 2006. Acceso al texto de la Sentencia en el siguiente enlace: http://hudoc.echr.coe.int/eng#{"itemid":["001-76114"]}

[309] Consejo de Europa. Tribunal Europeo de Derechos Humanos (sección segunda) Caso Biriuk vs. Lituania. Sentencia de 25 de octubre de 2008. Acceso al texto de la Sentencia en el siguiente enlace: http://hudoc.echr.coe.int/eng#{"itemid":["001-89827"]}

[310] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Gran Sala) Caso Rotaru vs. Rumanía. Sentencia de 4 de mayo de 2000. Acceso al texto de la Sentencia en el siguiente enlace: http://hudoc.echr.coe.int/eng#{"itemid":["001-58586"]}

derecho de acceso a los mismos en el caso *Godelli vs. Italy*[311], cuando la recurrente, abandonada al nacer en 1943 y habiendo dicho expresamente su madre biológica que se mantuviera en secreto su identidad, quería saber de sus orígenes alegando además el daño psicológico que le había causado en su infancia no saber de sus raíces. El TEDH consideró vulnerado el derecho a la vida privada porque la ley italiana no llevaba a cabo un adecuado equilibrio entre los intereses en juego y no había hecho uso de su margen de apreciación.

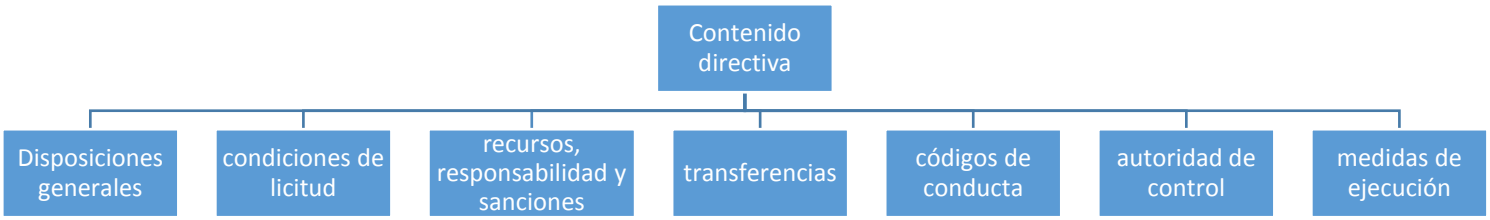
Para terminar con el plano jurisprudencial, se debe señalar, al igual que en el derecho a la intimidad, la aplicación en el ámbito concreto de la protección de datos, del juicio previsto en el artículo 8.2 CEDH a la hora de considerar si una injerencia ha vulnerado o no el referido derecho. Esto es, nos encontramos con la necesidad de que la injerencia por parte de la autoridad pública estuviera prevista por la ley, fuera necesaria en una sociedad democrática y tuviera una finalidad legítima. A título de ejemplo y como reflejo de esta idea, el citado caso *Uzun vs. Germany* en el que el Tribunal consideró que el seguimiento por GPS y el tratamiento de los datos obtenidos, si bien interferían en la vida privada, tenían una finalidad legítima, en este caso la protección de la seguridad nacional entre otras; había sido proporcionada, por cuanto solo se había recurrido a este sistema cuando métodos menos intrusivos se habían demostrado ineficaces; durante un corto periodo de tiempo y había afectado al recurrente solamente mientras viajaba en su coche; y considerando que afectaba a crímenes muy serios, se consideraba necesaria en una sociedad democrática.

Pero si hay un ámbito que merece nuestra atención, tanto por su trascendencia en sí mismo como porque va a constituir el punto de partida de nuestro trabajo, es el tratamiento y regulación que de esta materia se ha llevado a cabo en el seno de la Unión Europea. Como señala el Considerando 11 de la Directiva 95/46 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. "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". Es decir, se daba un paso más, de los principios al detalle, de lo general a lo concreto, del espacio internacional al mercado interior.

[311] Consejo de Europa. Tribunal Europeo de Derechos Humanos (sección segunda) Caso Godelli vs. Italia. Sentencia de 25 de septiembre de 2012. Acceso al texto de la Sentencia en el siguiente enlace: http://hudoc.echr.coe.int/eng#{"itemid":["001-113460"]}

Estábamos ante el punto de partida de la normativa que ha regido la protección de datos en Europa y que ha sido referencia en otras latitudes durante los últimos veinte años. Se pasaba a reflejar por un lado las distintas obligaciones que incumben a cualesquiera sujetos que efectúen tratamientos (la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control v las circunstancias en las que se puede efectuar el 'tratamiento); y, por otra parte, los derechos otorgados a las personas cuyos datos son objeto de tratamiento (ser informadas acerca de dicho tratamiento, poder acceder a los datos, poder solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias).

Son varios los argumentos que se esgrimieron para aprobar esta norma, y algunos de ellos, lógicamente, muy similares a los que en su día habían justificado el Convenio 108: el hecho de que se recurría cada vez más en la Comunidad al tratamiento de datos personales en los diferentes sectores de actividad económica y social; que el avance de las tecnologías de la información facilitaba considerablemente el tratamiento y el intercambio de dichos datos; o que las diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros por lo que respecta al tratamiento de datos personales, podían impedir la transmisión de dichos datos del territorio de un Estado miembro al de otro. Es decir, había un trasfondo económico en el impulso de esta normativa que resultaba lógico si se recuerdan los orígenes de la Unión europea. La norma, todavía vigente en el momento de escribir estas líneas, tiene la siguiente estructura:



Fuente: elaboración propia

Cada uno de estos puntos, que insistimos, constituye la base del régimen jurídico de la protección de datos de todos los Estados miembros y ha cumplido un papel fundamental con

una flexibilidad y capacidad de adaptación a las nuevas realidades digna de elogio. El siguiente gran estadio fue el refuerzo que vivió este derecho fundamental, como se ha visto al principio de este capítulo, cuando se incluyó expresamente en la Carta de Derechos Fundamentales de la Unión Europea. A pesar de la flexibilidad de la norma, de su moldeabilidad, fruto en gran medida por labor de adaptación que ha ido realizando la jurisprudencia, tanto europea como nacional, y la ingente labor del Grupo de Trabajo del artículo 29, era necesaria una reforma. Como ya tuvimos la oportunidad de exponer en otro lugar[312], la Comisión Europea basó la necesidad de esta reforma en un doble motivo[313]: por un lado las diferencias con las que se procedió a la implantación de la Directiva del año 1995 que provoca que hoy exista una gran divergencia entre las normativas de los diferentes Estados miembros, aunque cabría añadir que también en gran medida debido a su diferente aplicación y al mayor o menor rigor que las autoridades de control han tenido. En todo caso esa situación ha provocado una falta de eficacia en su objetivo último que es la protección de los datos personales[314]. En segundo lugar, no podemos olvidar los nuevos retos que plantean los inevitables avances tecnológicos como ocurre con el fenómeno de las redes sociales, la computación en nube[315], las tarjetas inteligentes o los denominados servicios basados en la localización; por no hablar de la proyección que pueden empezar a tener otras tecnologías como la denominada "Internet de las cosas", la robótica o la inteligencia artificial. Basta recordar algunos datos del año 1995 cuando se aprobó la primera Directiva para observar lo que han supuesto los avances tecnológicos[316]: la *World Wide Web* existía, pero solamente había 20.000 páginas Web en el mundo; no se podía utilizar Google, puesto que la compañía comenzó a operar en 1998; no se podía mandar un correo a través de un servicio web, puesto que algunos como Hotmail nacieron en 1996 y otros como Yahoo en 1997; las redes sociales no existían y la más conocida actualmente, Facebook, surgió en 2004; mientras que Amazon vendió su primer libro en julio de 1995, aproximadamente tres meses antes de que la Directiva fuera aprobada…Más allá de esta fundamentación material,

[312] VILLARINO MARZO, J., La Unión Europea ante los retos de la era digital. La reforma de la política europea de protección de datos, en PASCUA MATEO, F. (Dir.), *Derecho de la Unión Europea y el Tratado de Lisboa*, Dykinson, 2013, p. 561-597.
[313] EUROPEAN COMMISSION*,* Why do we need an EU Data Protection Reform? Disponible en web: http://ec.europa.eu/justice/data-protection/index_en.htm
[314] COMISIÓN EUROPEA. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. La protección de la privacidad en un mundo interconectado Un marco europeo de protección de datos para el siglo XXI. COM (2012) 9 final. Disponible en web: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:ES:PDF
[315] EUROPEAN COMMISSION, European Cloud Computing Strategy, https://ec.europa.eu/digital-single-market/en/european-cloud-computing-strategy
[316] PITT-PAYNE, T.*,* Data Protection the EU Reform Proposals [en línea]*, kbw,* 22 de febrero de 2012. Disponible en web: http://www.11kbw.com/uploads/files/DPTPPP.pdf p. 2

desde el punto de vista jurídico, la Comisión proponía que el nuevo marco constara de un Reglamento de ámbito general y una Directiva con un campo de actuación más reducido. Esto era posible porque el artículo 16 del Tratado de Funcionamiento de la Unión Europea consagra el derecho a la protección de dato como un derecho para cada individuo: "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por 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 estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes".

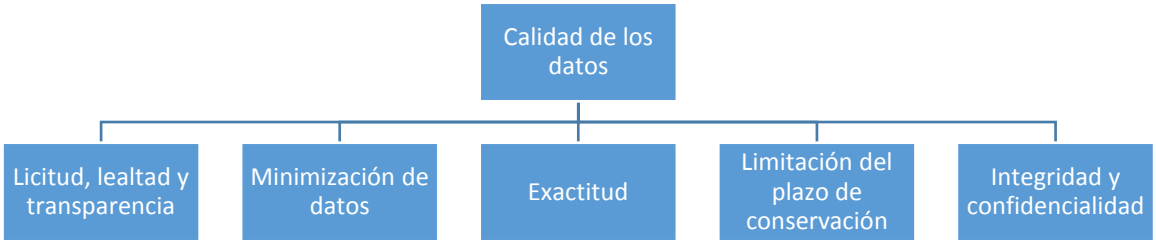
El proceso, que comenzó en el año 2012 con la presentación de la propuesta por parte de la Comisión Europea, culminó el pasado mes de mayo de 2016 con la publicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Desde el punto de vista de su contenido, y al margen de lo ya señalado más arribar a la hora de delimitarlo, se trata de un derecho que pretende satisfacer el bien jurídico de la autodeterminación informativa y que se concreta, siguiendo a Lucas Murillo de la Cueva, en tres puntos básicos: derechos y garantías para los titulares de los datos de carácter personal; las correlativas obligaciones de quienes tratan esos datos en lo que se refiere a la calidad y seguridad de los mismos y las oportunas restricciones en el acceso a dichos datos por parte de terceros[317].

Dentro de todo el contenido, por su particular trascendencia y considerando que en el resto de este trabajo, al hilo de tratar los aspectos propios de la privacidad en el entorno de la nube, se detallarán muchos otros, vamos a destacar y a detenernos, siquiera sucintamente, en el principio de calidad de los datos, por constituir el pilar que sostiene toda la normativa, su verdadero contenido esencial. La propia Comisión Europea lo resume como que "los datos personales serán tratados de manera leal y lícita, y recogidos con fines determinados,

[317] LUCAS MURILLO DE LA CUEVA, P., La construcción del derecho a la autodeterminación informativa, ob. cit,, p. 36.

explícitos y legítimos. Además, serán adecuados, pertinentes y no excesivos, exactos y, cuando sea necesario, actualizados, y deberán conservarse durante un período no superior al necesario y solo para los fines para los que fueron recogidos". Hoy día el RGPD sin una mención específica en el texto al principio de calidad, desglosa su contenido en un conjunto de principios tal y como refleja la siguiente figura:



Fuente: elaboración propia

La otra vertiente, de contenido activo, y con gran repercusión, es el haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, aspecto que, como se ha visto más arriba en pronunciamiento de nuestro TC, constituye el elemento diferenciador del derecho fundamental a la protección de datos con respecto al derecho a la intimidad. Como decía la Exposición de Motivos de la LORTAD, "los derechos de autodeterminación, de amparo, de rectificación y de cancelación los que otorgan virtualidad normativa y eficacia jurídica a los principios consagrados en la parte general, principios que, sin los derechos subjetivos ahora aludidos, no rebasarían un contenido meramente programático". En la actualidad, esto se concreta, sin entrar en disquisiciones conceptuales entre derechos y facultades, en un conjunto de derechos que la normativa europea concreta tanto en la Directiva como en el RGPD. Siguiendo a este último, los reflejamos en la siguiente figura:

Fuente: elaboración propia

Como resulta obvio, y más desde su inclusión expresa en la Carta de Derechos Fundamentales de la Unión Europea, el TJUE no ha sido ajeno a la realidad de la protección de datos y nos ha ido dando una abundante jurisprudencia sobre la materia, contribuyendo, insistimos, a que haya podido sobrevivir al paso de los años de una manera más que razonable. Al igual que en el caso del TEDH, el TJUE ha contribuido a fijar el concepto de dato personal y consiguientemente el ámbito de actuación de la normativa y de aplicación en definitiva de este nuevo derecho fundamental. Hay que partir en todo caso de la definición que hoy nos da el RGPD, muy similar, aunque actualizada, a la que nos daba la Directiva. Se considera dato personal "toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona". A partir de esta definición el TJUE[318] ha incluido por tanto algunos mencionados expresamente como el nombre (caso *Linquist*)[319], el apellido y el nombre de pila (caso *Tietosuojavaltuutettu vs. Satakunnan Markkinapörssi Oy* ya citado), las huellas dactilares (caso *Schwartz vs. Bochum*)[320], los datos de fichado en un trabajo (caso *Worten – Equipamentos para o Lar, S.A., vs. Autoridade para as Condições de Trabalho)*[321], la imagen de una persona (caso *Rynes vs. Urad pro ochranu osobnich udaju*)[322], los datos fiscales (caso *Bara vs. Președintele*

[318] La mayoría de las referencias jurisprudenciales recogidas del excelente compendio elaborado por la Oficina de Lucha Antifraude de la Unión Europea. LAUDATI, L., Summaries of EU Court Decisions relating to data protection 2000-2015, *European Anifraud Office,* 28 january 2015. Disponible en web: https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf

[319] Unión Europea. Tribunal de Justicia de la Unión Europea. Caso Lindquist. Sentencia de 6 de noviembre de 2003. Acceso al texto de la Sentencia en el siguiente enlace: http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=236011

[320] Unión Europea. Tribunal de Justicia de la Unión Europea (sala cuarta). Caso Schwartz vs. Bochum. Sentencia de 17 de octubre de 2013. Acceso al texto de la Sentencia en el siguiente enlace: http://curia.europa.eu/juris/document/document.jsf?text=&docid=143189&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=237516

[321] Unión Europea. Tribunal de Justicia de la Unión Europea (sala tercera). Caso Worten – Equipamentos para o Lar, S.A., vs. Autoridade para as Condições de Trabalho. Sentencia de 30 de mayo de 2013. Acceso al texto de la Sentencia en el siguiente enlace: http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:62012CJ0342&from=EN

[322] Unión Europea. Tribunal de Justicia de la Unión Europea (sala cuarta). Caso Rynes vs. Urad pro ochranu osobnich udaju. Sentencia de 11 de diciembre de 2014. Acceso al texto de la Sentencia en el siguiente enlace: http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:62013CJ0212&from=CS

Casei Naționale de Asigurări de Sănătate)[323], o la polémica en torno a las direcciones IP (caso *Scarlet vs. SABAM*)[324], que recientemente el TJUE ha vuelto a subrayar, incluidas las IP dinámicas, como verdaderos datos personales en el sentido de la Directiva (caso *Patrick Breyer vs Germany*)[325].

Al igual que hemos visto en el caso del TEDH, también el TJUE ha tenido la oportunidad de pronunciarse en muchas ocasiones sobre diversos aspectos del contenido de este nuevo derecho fundamental, tanto en lo que concierne al ciclo de vida de los datos, como en lo relativo al haz de facultades que corresponde a su titular. Pensemos por ejemplo como el TJUE ha llegado a señalar en la ya citada y muy conocida STJUE del caso *Costeja* que "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". También ha considerado tratamiento el subir datos personales a una página web (en el citado caso *Lindquist* o en el caso *Weltimmo s. r. o. vs. Nemzeti Adatvédelmi és Információszabadság Hatóság*)[326] o la filtración y posterior publicación de una nota de prensa (caso *Nikolaou vs. Comisión Europea*)[327].

En cuanto a las referidas facultades, el TJUE se ha pronunciado en diversas ocasiones. Así, el caso *Bara vs. Președintele Casei Naționale de Asigurări de Sănătate* antes citado en el

[323] Unión Europea. Tribunal de Justicia de la Unión Europea (sala tercera). Caso Bara vs. Președintele Casei Naționale de Asigurări de Sănătate. Sentencia de 1 de octubre de 2015. Acceso al texto de la Sentencia en el siguiente enlace: http://curia.europa.eu/juris/document/document.jsf?docid=168943&doclang=EN

[324] Unión Europea. Tribunal de Justicia de la Unión Europea (sala tercera). Caso Scarlet vs. SABAM. Sentencia de 24 de noviembre de 2011. Acceso al texto de la Sentencia en el siguiente enlace: http://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=238843

[325] Unión Europea. Tribunal de Justicia de la Unión Europea (sala segunda). Caso Patrick Breyer vs Germany. Sentencia de 19 de octubre de 2016. Acceso al texto de la Sentencia en el siguiente enlace: http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN&cid=1095511

[326] Unión Europea. Tribunal de Justicia de la Unión Europea (sala tercera). Caso Weltimmo s. r. o. vs. Nemzeti Adatvédelmi és Információszabadság Hatóság. Sentencia de 1 de octubre de 2015. Acceso al texto de la Sentencia en el siguiente enlace: http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=EN

[327] Unión Europea. Tribunal de Justicia de la Unión Europea (sala tercera). Caso *Nikolaou vs. Comisión Europea*. Sentencia de 12 de septiembre de 2007. Acceso al texto de la Sentencia en el siguiente enlace: http://curia.europa.eu/juris/document/document.jsf?text=&docid=62776&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=241700

que se consideró vulnerado el derecho a la información de los recurrentes tras el hecho de que la autoridad fiscal rumana había comunicado a la autoridad nacional de seguros de salud los datos sobre los ingresos de aquellos sin que tuvieran conocimiento de ello. O el caso *College van burgemeester en wethouders van Rotterdam vs. M.E.E. Rijkeboer*[328] en el que se subraya que el derecho de acceso a los datos es fundamental por cuanto permite al interesado ejercer sus otros derechos (rectificación, bloqueo, supresión, objeción al tratamiento o requerimiento de daños). A ellos habría que añadir también el derecho de supresión, que tuvo su máxima expresión en el denominado derecho al olvido plasmado en el caso *Costeja* que se acaba de citar.

Como ya se ha apuntado más arriba, España se puede considerar pionera en cuanto al reconocimiento del derecho a la protección de datos como derecho fundamental. El ya mencionado artículo 18.4 CE y la interesante exposición de motivos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, son una prueba de dicha afirmación. Actualmente la normativa española se recoge fundamentalmente en la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal. Desde el principio además nuestro Tribunal Constitucional le ha otorgado la categoría de derecho fundamental. Así lo hizo la STC 254/1993[329] que subraya que "estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de 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»" (F.J.6º), o la STC 94/1998 más arriba citada; pero también otras como la STC 202/1999[330] que hablaba del derecho a la libertad informática (F.J. 5º), término que el TC considera sinónimo del "derecho fundamental a la

[328] Unión Europea. Tribunal de Justicia de la Unión Europea (sala tercera). Caso College van burgemeester en wethouders van Rotterdam vs. M.E.E. Rijkeboer. Sentencia de 7 de mayo de 2009. Acceso al texto de la Sentencia en el siguiente enlace: http://curia.europa.eu/juris/document/document.jsf?text=&docid=74028&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=242871

[329] España. Tribunal Constitucional (sala primera). Sentencia 254/1993 de 20 de julio de 1993. Acceso al texto de la Sentencia en el siguiente enlace: https://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_constitucional/common/pdfs/13._Sentencia_254-1993_de_20_julio_1993._def_-_copia.pdf

[330] España. Tribunal Constitucional (sala primera). Sentencia 202/1999 de 8 de noviembre de 1999. Acceso al texto de la Sentencia en el siguiente enlace: https://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_constitucional/common/pdfs/9._Sentencia_202-1999_de_8_de_noviembre_de_1999._def.pdf

protección de datos personales frente a la informática" (STC 290/2000[331], F.J.7º), o del derecho a la "autotutela informativa" (STC 29/2013, F.J.4º)[332] que definía como el "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 aquél legítimo que justificó su obtención" (F.J.2º). Es también la STC 202/1999 la que nos dice el contenido del derecho fundamental a la protección de datos "consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente 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" (F.J.7º).

Se refleja claramente en esta Sentencia tanto el pilar del principio de calidad de los datos como la vertiente subjetiva concretada en los derechos de los que es titular el interesado; al igual que hace la STC 29/2013 que recuerda que se vulnera el derecho fundamental a la protección de datos cuando se utilizan de manera no consentida ni previamente informada unas grabaciones para un fin desconocido por el afectado (F.J.4º).

Es también la Sentencia 202/1999, la que hace referencia a los límites al referido derecho, que pueden ser restricciones directas del derecho fundamental mismo o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental (F.J.11º). A su vez añade que "Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas

[331] España. Tribunal Constitucional (pleno). Sentencia 290/2000 de 30 de noviembre de 2000. Acceso al texto de la Sentencia en el siguiente enlace: http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_constitucional/common/pdfs/Sentencia290.pdf

[332] España. Tribunal Constitucional (sala primera). Sentencia 29/2013 de 11 de febrero de 2013. Acceso al texto de la Sentencia en el siguiente enlace: http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_constitucional/common/pdfs/SENTENCIA_29-2013_de_11_de_febrero__de_2013.pdf

que hagan previsible al interesado la imposición de tal limitación y sus consecuencias" (F.J.16º); y que como señala la STC 17/2013 [333] "han de respetar su contenido constitucionalmente declarado y encontrar su fundamento en otros bienes o derechos constitucionalmente protegidos".

3.3.2 Breve referencia al derecho a la protección de datos fuera de Europa

Fuera de nuestras fronteras continentales, la reflexión sobre la existencia de un derecho fundamental ha tenido perspectivas diferentes. En el caso de EE.UU, no existe propiamente una normativa comprensiva del derecho a la protección de datos. A pesar de que firmó en 1981 las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales, no los ha implantado en su ordenamiento interno. En lugar de eso y más allá de la ECPA, ha llevado a cabo un tratamiento sectorial con una combinación de legislación y autorregulación[334]. En esta línea ya en el año 1998 Lessig apuntaba que los Estados Unidos han actuado tradicionalmente bajo la doctrina del *laissez-faire* en materia de privacidad. La regulación americana -decía este autor- es esporádica y parcial, incompleta desde la perspectiva de la privacidad de los datos en Europa[335].

Más allá de las disquisiciones conceptuales respecto a la correcta traducción del "right to privacy", en puridad existen claras diferencias sobre la política legislativa en materia de protección de datos en Estados Unidos y en Europa. Siguiendo a Piñar Mañas, podemos señalar como las más relevantes las siguientes[336]: por un lado, en Estados Unidos se ha optado por la autorregulación y la proliferación de códigos de conducta, mientras que en Europa se ha optado por la heterorregulación y por la consideración del derecho a la protección de datos como un verdadero derecho fundamental; por otro, en Estados Unidos no ha considerado necesaria una autoridad de control independiente, aunque hay Agencias como la *Federal Trade Commisiion* que tiene algunas competencias, frente al carácter esencial de dicho órgano en el marco europeo.

[333] España. Tribunal Constitucional (Pleno). Sentencia 17/2013 de 31 de enero de 2013. Acceso al texto de la Sentencia en el siguiente enlace: https://www.boe.es/boe/dias/2013/02/26/pdfs/BOE-A-2013-2167.pdf
[334] Por ejemplo ha sido particularmente incisiva en el ámbito sanitario a través de los Standards for Privacy of Individually Identifiable Health Information (2000) y los Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule) under the Health insurance Portability and Accountability Act o f 1998 (HIPAA).
[335] LESSIG, L., ob. cit., p. 13
[336] LUCAS MURILLO DE LA CUEVA, P. y PIÑAR MAÑAS, J.L., ob. cit., pp. 177 y 178.

En Iberoamérica[337], al igual que ocurre en muchos otros ámbitos, nos encontramos con diversas vías a través de las cuales se ha reconocido la existencia de un derecho fundamental a la protección de datos. Así, nos encontramos con países en los que hay un reconocimiento constitucional, sea de la sustantividad del derecho fundamental en sí mismo como en la Constitución de Ecuador cuyo artículo 66.19 dice que "Toda persona tiene: El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley" o en la Constitución de México tras la reforma de 2008 que recoge en el párrafo segundo de su artículo 16 que "toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros"; o sea la vertiente garantista de otros derechos fundamentales. Es el caso por ejemplo de Colombia, el artículo 15 de su Constitución dice en su segundo inciso que "De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas". En el caso de la Constitución Hondureña, contemplado dentro del título referido a las Garantías Constitucionales, se recoge el habeas data, que se contempla "Para obtener acceso a la información; impedir su transmisión o divulgación; rectificar datos inexactos o erróneos; actualizar información, exigir confidencialidad y la eliminación de información falsa; respecto de cualquier archivo o registro, privado o público, que conste en medios convencionales, electrónicos o informáticos, que produzcan daño al honor, a la intimidad personal, familiar y a la propia imagen. Esta garantía no afectará el secreto de las fuentes de información periodística". Digno de mención es el caso venezolano [338] , donde la jurisprudencia ha llevado a cabo el recorrido de partir originariamente del reconocimiento de la vertiente garantista (habeas data) entre otras en la

[337] LÓPEZ CARBALLO, D.A. (Coord.), *Protección de datos y habeas data: una visión desde Iberoamérica*, Agencia Española de Protección de Datos, 2015, 218 p. Disponible en Web: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/premios_2015/Proteccion_de_datos_y_habeas_data.pdf

[338] RODRÍGUEZ MARCA, E., *El derecho fundamental a la protección de datos de carácter personal en Venezuela y su desarrollo desde la Sala Constitucional del Tribunal Supremo de Justicia [en línea]* Red Iberoamericana de protección de datos. 15 de septiembre de 2015. Disponible en web: http://www.redipd.org/noticias_todas/2015/tribuna/news/15_09_2015-ides-idphp.php

Sentencia de 31 de agosto de 2000[339], pasando por la asunción del derecho a la autodeterminación informativa en la Sentencia de 15 de diciembre de 2005[340] que señala "tiene como consecuencia el control que posee cada ciudadano frente a la información que les concierne personalmente, sea íntima o no, para preservar de este modo y en último extremo la propia identidad, dignidad y su libertad ante las injerencias en la zona espiritual íntima y reservada de una persona o un grupo, especialmente de una familia, la cual comprende no sólo sus relaciones afectivas o sexuales, sino también la esfera de confianza que abarca toda la información de un sujeto como afinidad o parentesco, entre otras", hasta llegar a una visión integradora de ambas vertientes en su Sentencia de 4 de agosto de 2011[341] al señalar que "La concepción del derecho a la protección de datos de carácter personal, trasciende entonces el resguardo del ámbito íntimo de la vida privada, y alcanza la posibilidad de controlar esa información, a los fines de asegurar a las personas frente al riesgo que supone el acopio y transmisión de sus datos, como una cuestión que en muchos casos se extiende (más allá del interés particular) a la necesidad de la sociedad en general de contar con medios que la protejan, ante el uso indebido de su información, la cual puede conducir a la negación de derechos fundamentales -vgr. participación- o en la ineficacia de las instituciones que hacen posible su ejercicio".

En otras ocasiones, al margen de la proyección legislativa, han sido los tribunales los que también han contribuido a su reconocimiento, delimitación y consolidación. Además del ejemplo venezolano que acabamos de transcribir, recientemente por ejemplo el Tribunal Constitucional de la República Dominicana, en su Sentencia de 18 de octubre de 2016, señalaba que "toda persona tiene derecho a que los datos personales que una institución pública o privada conserva se mantengan en estricto secreto y que solo sean utilizados con apego a los fines para los cuales fueron almacenados. Por otra parte, el titular de dichos

[339] Venezuela. Tribunal Supremo de Justicia (Sala Constitucional). Sentencia nº 1053 de 31 de agosto de 2000. Acceso al texto de la Sentencia en el siguiente enlace: http://jurisprudencia.vlex.com.ve/vid/willian-ojeda-orozco-283518283ç

[340] Venezuela. Tribunal Supremo de Justicia (Sala Constitucional). Sentencia nº 4975 de 15 de diciembre de 2005. Acceso al texto de la Sentencia en el siguiente enlace: http://historico.tsj.gob.ve/decisiones/scon/diciembre/4975-151205-05-0952.HTM

[341] Venezuela. Tribunal Supremo de Justicia (Sala Constitucional). Sentencia nº 1318 de 4 de agosto de 2011. Acceso al texto de la Sentencia en el siguiente enlace: http://jurisprudencia.vlex.com.ve/vid/german-jose-mundarain-hernandez-311569838

datos tiene el derecho a conocerlos, y requerir la corrección de los que no se correspondan con la realidad"[342].

Y también para establecer sus límites[343]. Así el Tribunal Superior Federal de Brasil, en su Sentencia de 8 de julio de 2009[344], se pronunció en un caso que involucraba la demanda de un sindicato de empleados estatales contra la decisión del alcalde de Sao Paulo de revelar a través del internet los nombres, puestos y salarios de los 147.000 empleados de esa alcaldía y de 15.000 personas contratadas por la ciudad. El tribunal, aplicando la técnica de ponderación de derechos, consideró que el principio de máxima divulgación de la información pública debería prevalecer por sobre el derecho a la protección de datos y subrayó la importancia de internet para el control de las cuentas públicas.

Observamos por tanto que, a través de diversos mecanismos jurídicos, normativos o jurisprudenciales, se ha ido dando un progresivo reconocimiento del derecho a la protección de datos como un verdadero derecho fundamental y que, siguiendo a la Agencia Española de Protección de datos, podemos definir como un derecho fundamental que reconoce al ciudadano la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos[345]. En conclusión, en línea con la evolución de las últimas décadas, podemos decir que la regulación del derecho a la protección de datos ha de ser principialista, siendo el principio de calidad de los datos el eje sobre el que gire su regulación. Ello sin perjuicio del importante papel de adaptabilidad que han jugado –y que deben seguir jugando– las autoridades de protección de datos, la jurisprudencia y la propia industria. Al hilo de la segunda parte de este trabajo, donde analizaremos con detalle muchos aspectos del régimen jurídico de la protección de datos, veremos si esta forma de aproximación normativa resulta válida también para el entorno de la computación en nube.

---

[342] República Dominicana. Tribunal Constitucional. Sentencia TC/0484/16 de 18 de octubre de 2016. Acceso al texto de la Sentencia en el siguiente enlace: http://progresomicrofinanzas.org/wp-content/uploads/2016/12/republica-dominicana-sentencia-tc-reforma-ley-habeas-data-1.pdf

[343] CORTE INTERAMERICANA DE DERECHOS HUMANOS. Relatoria Especial para la Libertad de Expresión. *El derecho de acceso a la información en el marco jurídico interamericano*. 2010. Disponible en web: http://www.oas.org/es/cidh/expresion/docs/publicaciones/ACCESO%20A%20LA%20INFORMACION%20FINAL%20CON%20PORTADA.pdf

[344] Brasil. Tribunal Superior Federal. Sentencia de 8 de julio de 2009. Acceso al texto de la Sentencia en el siguiente enlace: http://right2info.org/resources/publications/Brazil%20S.Ct%20salarios%20SP%20Jul%202009.pdf

[345] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía del derecho fundamental a la protección de datos. 2004. Disponible en web: https://www.agpd.es/portalwebAGPD/common/FOLLETO.pdf

“Creo que hay un mercado mundial para quizás cinco ordenadores”

Thomas J. Watson, antiguo Presidente de IBM

“640 Kilobytes es más memoria de la que nadie nunca podrá necesitar”

Bill Gates, fundador de Microsoft

“I don't need a hard disk in my computer if I can get to the server faster... carrying around these non-connected computers is byzantine by comparison”

Steve Jobs, Apple

CAPÍTULO II: EL *CLOUD COMPUTING* DESDE EL PUNTO DE VISTA TECNOLÓGICO Y ECONÓMICO, Y LOS DESAFÍOS DE ESTA TECNOLOGÍA.

1 El cloud computing desde el punto de vista tecnológico

En el presente capítulo tal y como se ha explicado en la introducción de este trabajo, vamos a definir en qué consiste el *cloud computing* , el contexto y los motivos por los que se origina, así como sus características descriptivas desde el punto de vista tecnológico, con la finalidad de comprender de qué estamos hablando. Su particular vinculación al negocio, que explica en gran medida el éxito que ha tenido frente a otras modalidades de computación previas, exigirá también analizar la vertiente económica, tanto desde el punto de vista macroeconómico, como desde el punto de vista de sus beneficios para la empresa.

Sin embargo, un capítulo que trata de realizar un acercamiento a los orígenes de la computación en nube, su desarrollo, sus principales ventajas y sus repercusiones económicas, no estaría completo si no incluyera una referencia a lo que muchos han calificado como riesgos, sin perjuicio de que los riesgos son inherentes a cualquier actividad y máxime a cualquiera que esté relacionada con el mundo tecnológico.

Estas reflexiones resultan necesarias, ya que si no se reconoce a la computación en nube una dimensión tecnológica propia y una proyección económica, carecería de justificación entrar a analizar en qué medida el actual régimen jurídico del derecho a la protección de datos resulta válido en este nuevo entorno.

1.1 Definición y características.

Señalaba la Comisión Europea, que el *cloud computing* es un concepto/paradigma[346] y reconoce que no puede dar un concepto completo sino *representativo*[347]. Estamos ante un concepto que originariamente recibió muchas definiciones: así, la consultora Gartner lo define como un estilo de computación que capacita a la TI para proveer servicios a múltiples usuarios externos vía Internet de forma masiva y escalable; Forrester subraya que el cloud provee infraestructura TI gestionada de forma abstracta, altamente elástica y escalable, capaz de hospedar a las aplicaciones del usuario final y de facturar según el consumo realizado; la Revista Cloud Computing lo define como "un nuevo concepto tecnológico que se basa en que las aplicaciones software y los equipos hardware con capacidad de proceso y almacenaje de datos no están en el PC o equipos del usuario, sino que están ubicados en un *Datacenter* que permite a los usuarios acceder a las aplicaciones y servicios disponibles a través de Internet o como se conoce coloquialmente a través "la Nube" de Internet, de una forma sencilla y cómoda"[348]; mientras que la Agencia Española de Protección de Datos señala que es una nueva forma de prestación de los servicios de tratamiento de la información, válida tanto para una empresa como para un particular y, también, para la Administración Pública[349]. Incluso contamos con una definición auténtica, ya que el artículo 3.VI de la Ley General de Protección de Datos Personales en posesión de sujetos obligados de México define el cómputo en la nube (versión de 26 de enero de 2017) como "Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente".

En el plano doctrinal, Vaquero, Rodero, Cáceres y Línder lo definen como "un amplio *pool* de recursos virtualizados accesibles y fácilmente utilizables (como hardware, plataformas de desarrollo y/o servicios). Estos recursos pueden ser reconfigurados para ajustarse a un peso variable (escala), permitiendo también una utilización óptima de los recursos. Este *pool* de

---

[346] EUROPEAN COMMISSION. Expert Group Report*, The Future of Cloud computing. Opportunities for European Cloud computing Beyond 2010.* 2010. 66 p. Disponible en web: http://cordis.europa.eu/fp7/ict/ssai/docs/*cloud*-report-final.pdf,

[347] *Idem*, p. 8. En este mismo documento la Comisión Europea afirma directamente que la nube no se refiere a una tecnología específica sino a un paradigma de aprovisionamiento general con capacidades mejoradas, p. 12.

[348] La Revista Cloud Computing dispone de un glosario de términos donde se recoge esta definición. Disponible en web: http://www.revistacloudcomputing.com/glosario-cloud-computing/#

[349] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía para clientes que contraten servicios de Computing. 2013. Disponible en web: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf

recursos está típicamente explotado por un modelo de pago por demanda en el que las garantías son otorgadas por el proveedor de infraestructuras a través de un Acuerdo de Nivel de Servicio a medida"[350].

A pesar de esta diversidad, informada ciertamente por muchas similitudes, y de que la OCDE califica metafóricamente el concepto de *cloud* (nube) como "*cloudy"* (nuboso) [351] progresivamente existe un cierto consenso respecto a la utilización de la definición dada por el Instituto Nacional para los Estándares y la Tecnología de Estados Unidos (NIST en su acrónimo inglés) que ha definido la computación en nube o computación en la nube, como un modelo de computación que permite conectar un acceso a la red ubicuo, adecuado y bajo demanda a un conjunto de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente provistos y retirados con un mínimo esfuerzo de gestión o de interacción del proveedor de servicios[352]. Con base en esta definición provista por el NIST, se pueden señalar cuáles son las principales características de esta nueva tecnología[353]:

- Elasticidad rápida: para el consumidor, la nube aparece como algo infinito y puede adquirir más o menos poder de computación como necesite. A título de ejemplo, el cliente elimina la necesidad de "sobreaprovisionamiento" para alternar picos de demanda con períodos en los que los recursos no están en uso[354].
- Servicio a medida: en un tipo de servicio de esta naturaleza, aspectos del servicio en nube son controlados y supervisados por el prestador del servicio, algo que es

[350] VAQUERO, L.M., RODERO-MERINO, L., CÁCERRES, J. y LINDER, MAIK. A Break in the Clouds: Towards a Cloud Definition. *Computer Communication Review.* enero de 2009, Vol. 39, nº 1. ftp://doc.nit.ac.ir/cee/jazayeri/research%20method/a%20break%20in%20the%20*cloud*s%20towards%20a%20*cloud*%20definition.pdf

[351] OECD. Cloud Computing: The Concept, Impacts and the Role of Government Policy. *OECD Digital Economy Papers*. 2014. nº. 240, Paris. Disponible en web: http://dx.doi.org/10.1787/5jxzf4lcc7f5-en

[352] MELL, P. y GRANCE, T., The NIST definition of Cloud computing (Draft), Recommendations of the National institute of Standards and Technology. *National institute of Standards and Technology (NIST), Special-Publication.* Enero 2011, Disponible en web: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
Por su parte Neelie Kroes, Vicepresidenta de la Comisión Europea señaló en el Foro de Davos el 27 de enero de 2011 que "Respecto de la computación en nube, me he dado cuenta de que no podemos esperar una definición que sea aceptada por todos".

[353] RAYPORT, J.F. y HEYWARD, A. Envisioning the Cloud: The Next Computing Paradigm [en línea]. *Marketspace.* 20 de marzo de 2009. Disponible en web: http://www.hp.com/hpinfo/analystrelations/Marketspace_090320_Envisioning-the-*Cloud*.pdf,

[354] FUNDACIÓN DE LA INNOVACIÓN BANKINTER y ACCENTURE. Cloud computing. La tercera ola de las Tecnologías de la Información. 2010. p. 22, http://www.fundacionbankinter.org/system/documents/8156/original/XIII_FTF_*Cloud*Computing.pdf

fundamental para la facturación, el control de acceso, la optimización de recursos, la planificación y otros aspectos.

- Autoservicio bajo demanda: lo que significa que el consumidor puede usar los servicios en nube conforme a sus necesidades sin ninguna interacción humana con el prestador de servicios.
- Acceso universal a la red: lo que significa que las capacidades del prestador de servicios están disponibles en la red y se puede acceder a ellas a través de mecanismos estándar por cualquier cliente.
- Agrupación de recursos independiente de la ubicación o asignación dinámica: lo que supone que los recursos físicos y no físicos del prestador son asignados y reasignados en función de la demanda de los consumidores. La ubicación de los recursos físicos por debajo de la infraestructura de la nube no es conocida por el cliente y puede cambiar de manera dinámica. El estudio elaborado por IBM define este ocultamiento como *masked complexity* (complejidad oculta). Apunta la prestigiosa multinacional americana que se trata además de una nota característica que se proyecta económicamente puesto que permite aumentar la "sofisticación del producto o servicio vendido al consumidor sin requerir de mayores conocimientos por parte del usuario[355].
- Dispositivos más sencillos[356]: con la nube, los usuarios no necesitan un ordenador potente: una PDA, un teléfono móvil, una video consola e incluso sensores en la propia ropa[357] son suficientes para acceder a los servicios facilitados por la nube.

Desde el punto de vista histórico, cualquier acercamiento en materia de nuevas tecnologías tiene el gran inconveniente de que suele ser una historia muy reciente debido a la constante innovación y desarrollo que existe en este sector. Tal y como se ha podido observar en el capítulo anterior, se puede hablar de que cada año tenemos una verdadera revolución tecnológica que si lo catalogamos cada diez años nos sitúa con los *mainframes* en la década

[355] IBM INSTITUTE FOR BUSINESS VALUE. The power of cloud. Driving business model innovation. Febrero 2012. p. 6. Disponible en web:.http://public.dhe.ibm.com/common/ssi/ecm/en/gbe03471usen/GBE03471USEN.PDF

[356] Esta última nota no viene incluida en el listado del NIST sino que esta nota característica es aportada por la Dra. Cavoukian. CAVOUKIAN, A. Privacy in the clouds. A White Paper on Privacy and Digital Identity: Implications for the Internet. *Information and privacy commissioner of Ontario*. 30 p. Disponible en web: https://www.ipc.on.ca/wp-content/uploads/2008/05/privacyintheclouds.pdf

[357] Conectaría con la nueva fase tecnológica que se está desarrollando actualmente, conocida como Internet de las cosas (IoT en sus siglas inglesas).

de los sesenta, las minicomputadoras en los setenta, los PC en los ochenta los teléfonos móviles en los noventa, los *smart phones* en la década anterior…etc.

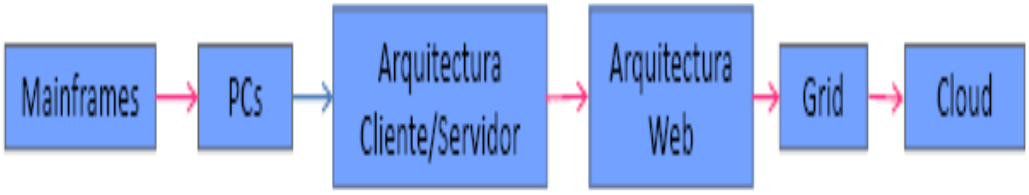
El caso del *cloud computing* no es diferente. En realidad, como afirman Rayport y Heyward[358], miembros de la firma de investigación Marketspace, la propia noción de *cloud computing* es, a la vez, familiar y radical. Familiar porque en sus orígenes los recursos compartidos estaban al orden del día y de ello hay buenos ejemplos[359]: así una de las grandes motivaciones para Internet y para Arpanet fue compartir recursos. Internet surgió en la época del *time-sharing*, y la pronta implantación del TCP fue hecha para grandes sistemas de tiempo compartido como Tenex y TOPS 20. Antes de que la tecnología semiconductora hiciera los ordenadores más pequeños, poderosos y económicos, lo que existía eran ordenadores *mainframes*. Como consecuencia del coste de estas últimas máquinas, surgían incentivos a los usuarios para compartirlas, accediendo a los servicios de computación a través de "terminales tontas" (*dumb terminals*) sobre las líneas de teléfono con base en un sistema de "compartir el tiempo" *(time-sharing*). En aquella época por tanto, el ordenador (el prestador del servicio) era todopoderoso, y la terminal (el cliente) estaba enormemente limitada en cuanto a lo que podía hacer. En la mayoría de los casos, señalan los citados autores, los terminales no disponían de poder de procesamiento y no tenían memoria. Con el paso de los *mainframes* a los miniordenadores en los años setenta, y el posterior paso a los ordenadores personales en los años ochenta y noventa, el procesamiento y el almacenamiento devinieron distribuidos. Precisamente la generalización de los ordenadores personales permitió el paso al conocido como modelo distribuido, en el que los usuarios individuales poseían un completo equipamiento de recursos informáticos "en una caja". Ya no era necesario por tanto acceder a un poder de computación central y de almacenamiento de una máquina compartida más grande o de un grupo de máquinas.

Pero también es algo radical. Efectivamente, a mediados de los noventa, la explosión de Internet [360] cambió de nuevo el paradigma de computación. La popularización y comercialización de Internet a través de la *World Wide Web* hizo Internet amigable para el consumidor, donde este y las empresas podían conectarse, comunicarse y hacer negocios. La web hizo del otrora arcano Internet –anteriormente de dominio exclusivo para las universidades, los gobiernos y los científicos- una realidad que llamaba al mercado de

[358] [358] RAYPORT, J.F. y HEYWARD, A. Ob. Cit.
[359] INTERNET SOCIETY. Brief History of the Internet. Disponible en web: http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet
[360] Nos remitimos a lo expuesto en el primer capítulo de esta obra y en particular a la obra de Janet Abbate.

masas. Si a ello sumamos la aparición en los noventa de los prestadores de servicios de Internet comerciales, que hicieron las conexiones online ampliamente accesibles, y más recientemente, con el surgimiento de prestadores de banda ancha, proveyeron la alta velocidad, las conexiones "*always on*" a través de líneas de servicio digital (DSL) ofrecidas por la grandes compañías de teléfonos, y los módems de cable ofrecidos por los operadores de televisión por cable, la referida explosión estaba asegurada.

La presencia de esas conexiones "*always on*" de alta velocidad cambió también la forma en que los usuarios se relacionan con su ordenador. Los patrones propios de las lentas conexiones telefónicas requerían de poderosas capacidades de computación a las máquinas y solamente pequeñas ráfagas de datos intercambiados a través de la red. Con el advenimiento de la banda ancha, estos patrones se intercambiaron. Ahora una enorme cantidad de datos podrían circular por y hacia la red, lo cual supone un cambio que requiere de menos datos, software y aplicaciones residiendo en nuestros ordenadores. A ello se suma la virtualización que consiste precisamente en que las aplicaciones ya no están sujetas a restricciones físicas, es decir, que no es necesario que se encuentren en el mismo lugar que la infraestructura informática. Esto permite que los servidores sean compartidos por muchas aplicaciones, al tiempo que las aplicaciones son susceptibles de ser ejecutadas virtualmente desde cualquier lugar[361]. Dotados de un acceso de banda ancha, los consumidores pueden aprovechar los recursos de la Web en busca de nuevas herramientas y servicios. Y aquí, en este contexto de acceso y generalización de los recursos Web o servicios de computación remota (*Web Services)*, es donde surge en 1999 Salesforce pionera en la oferta de aplicaciones empresariales a través de una sencilla web y, fundamentalmente, en 2002, *Amazon Web Services* que convierte a esta empresa en la pionera del entonces todavía incipiente mundo del *cloud computing*[362]. En el siguiente gráfico se ve la evolución a la que nos hemos referido.



[361] FUNDACIÓN DE LA INNOVACIÓN BANKINTER y ACCENTURE. Ob. Cit. p. 28.
[362] GARCÍA MEXÍA, P. *Historias…* Ob. Cit., p. 116.

Fuente: Carmen Costilla, “Foro sobre *Cloud computing*”, 15 de abril de 2010[363]

Fuente: elaboración propia

En los últimos años esta pauta de acceso a los recursos Web se ha desarrollado hasta completar, como dicen Rayport y Heyward, un círculo que provoca que para muchos usuarios el ordenador personal se haya convertido en un terminal, emergiendo como una simple puerta de entrada a la red[364], una más. Así lo subraya también el tecnólogo Clay Shirky al afirmar que “lo que está impulsando este cambio es el cambio de perspectiva de pasar de

[363] Hay quienes opinan que en cierta medida el *cloud computing* supone una vuelta a este modelo clásico en el que la nube se puede equiparar con un gran mainframe al que los usuarios acceden de forma remota desde sus propios terminales. FUNDACIÓN DE LA INNOVACIÓN BANKINTER y ACCENTURE, ob. cit., p. 38.

[364] Chris Anderson, editor jefe de la revista Wired afirmaba puntualizando y de modo provocador que lo importante en realidad en la actualidad es Internet y no la World Wide Web puesto que “pasamos el día en Internet, pero no en la Web”. ANDERSON, C. The Web Is Dead. Long Live the Internet. *Wired.* http://www.wired.com/magazine/2010/08/ff_webrip/ Este mismo autor señala en ese artículo que hoy día el mercado ha hablado y que, contrariamente a lo ocurrido a principios de los noventa en la guerra que las “telecos” perdieron frente a una “red tonta”, en lo concerniente a las aplicaciones que se encuentran en la Red, la gente ha comenzado a preferir la calidad del servicio. En la misma línea se puede situar la exitosa historia de Amazon. Ver GARCÍA MÉXIA, P. *Historias*…, ob. cit., p. 114 y siguientes.
Hace ya tiempo por su parte que Salesforce hizo famosa la frase “*The network is the computer*”.

ver el ordenador como una caja a pasar a verlo como una puerta". En 2009 Lee Gomes and Taylor Buley publicaban un artículo en Forbes titulado "*The Death of the PC*" y lo achacaban a la fusión de la informática en la nube y la virtualización, dando lugar a un nuevo ordenador que denominaban "*think computer"* caracterizado por una pantalla y un teclado pero con el proceso, los cálculos y las aplicaciones ejecutándose en un gran centro de datos[365]. Y fue el genial Steve Jobs quien el 1 de junio de 2009, en una conferencia en la Universidad del Sur de California, proclamó la era "post-PC"[366]. Estamos en línea con un fenómeno que se puede remontar a Licklider y su idea de la red de ordenadores intergaláctica[367] y que ya predijo de manera más concreta David Gelernter en 1991 en su obra *Mirror Worlds*[368], al describir realidades hoy cotidianas: las páginas web, el *blogging*, la realidad virtual, el video en *streaming*, las tabletas, los libros electrónicos los motores de búsqueda o la telefonía por Internet.

Vivimos una transformación consistente en el suministro de aplicaciones a través de la red (software como los programas del tipo Word o PowerPoint que normalmente utilizan los ordenadores), plataformas (entornos de computación o sistemas operativos tales como Windows o Linux) e infraestructura (poder de procesamiento y capacidad de almacenamiento). Los prestadores de servicios en nube están vaciando los ordenadores, lo que conlleva además una creciente utilidad de otro tipo de dispositivos que disponen de acceso a la red tales como los notebooks o los *smart phones*¸ de menor tamaño, menos consumo energético y menos precio. Como señala en una conocida metáfora Nicholas Carr[369], se puede comparar la revolución tecnológica que supone el cloud con la revolución que hubo a fines del siglo XIX cuando las fábricas dejaron de producir su propia electricidad a través de sus motores de vapor y sus dinamos y pasaron a conectarse a la red eléctrica.

La generalización de este fenómeno conlleva el surgimiento de lo que algunos han denominado sociedad ubicua. En la culminación de este proceso se encuentra en realidad la Internet de las cosas o lo que los profesores Murakami y Fuyinuma han denominado "Red

[365] GOMES, L. y BULEY, T. The Death of the PC. *Forbes.* 2009, Vol. 194, número 12. Disponible en web: http://www.forbes.com/forbes/2009/1228/technology-virtualization-vmware-wyse.html
[366] Acceso a la parte del video de la Conferencia en la que Steve Jobs usa esa expresión en el siguiente enlace: https://www.youtube.com/watch?v=YfJ3QxJYsw8
[367] LICKLIDER, J.C.R. *Memorandum for: Members and Affiliates of the Intergalactic Computer Network* [en línea]. 23 de abril de 1963. Disponible en web: http://worrydream.com/refs/Licklider-IntergalacticNetwork.pdf
[368] GELERNTER, D. *Mirror Worlds Or the Day Software Puts the Universe in a Shoebox...How It Will Happen and What It Will Mean*. 1st ed. Oxford University Press. 1992. 256 p.
[369] CARR, N. *The Big Switch: Rewiring the World, from Edison to Google.* W. W. Norton. 2008. 224 p.

Ubicua" y que consiste en un nuevo entorno TIC marcado por la interacción de redes, equipos y dispositivos de información, plataformas, contenidos y servicios[370].

Fuente: Bringing IoT and Cloud Computing towards Pervasive Healthcare[371]

Pero la descripción que se ha hecho del desarrollo tecnológico que ha acabado en el *cloud computing* no está exenta de polémicas y debates. No faltan quienes consideran que el *cloud computing* no es sino un nuevo término para un viejo sueño de la computación como

[370] MURAKAMI, T. y FURIYUMA, A. Ubiquitous Networking: Towards a New Paradigm.. *Nomura Research Institute Papers*. 2001, nº 2, p. 1-7. Disponible en web: https://www.nri.com/global/opinion/papers/2000/pdf/np200002.pdf

[371] DOUKAS, C. y MAGLOGIANIS, I. Bringing IoT and Cloud Computing towards Pervasive [en línea] . *IMIS.* 2012. Disponible en web: https://pdfs.semanticscholar.org/4132/551dc6a891c62979c4f2c8a07f5d5cc90b6d.pdf?_ga=1.149196341.2024153542.1483012606

utilidad que ha emergido como una realidad comercial[372]. Así opinaba por ejemplo en 2008 el CEO de Oracle cuando afirmaba en el *Wall Street Journal* "Lo interesante del *cloud computing* es que lo hemos redefinido para incluir todo lo que ya hacíamos…"; o también Richard Stallman, el defensor del software libre que afirmaba con rotundidad que "es una estupidez. Es más que una estupidez: es una hiper campaña de marketing"[373]. Hay autores que sostienen que el concepto de "cloud" es evolución de otros conceptos que ya existían en el mundo de la informática desde hace bastantes años[374].

Algunos proveedores efectivamente consideran que la computación en nube es en realidad el resultado de la convergencia de tres tendencias prominentes: en primer lugar, el Software as a Service (SaaS) que permite la utilización de aplicaciones a discreción del consumidor, quien sólo debe abonar una suscripción; en segundo lugar la virtualización por la cual, como hemos visto más arriba, las aplicaciones se separan de la infraestructura; y en tercer lugar el *utility computing*, donde el acceso a los servidores requeridos por un negocio se ofrece como un servicio de suministro más, pagando por uso[375], en la idea que antes hemos apuntado de Carr y que en realidad tiene su origen en la conferencia de John McCarthy en el MIT Centennial in 1961 donde pronunció su famosa frase de que "la computación podría algún día organizarse como un servicio público al igual que el sistema de telefonía es un servicio público".

También algunas instituciones señalan que la computación en nube no supone una nueva industria ni un salto revolucionario. El Consejo Económico y Social de la Unión Europea, en su dictamen publicado a principios de 2012 afirmaba que la computación en nube consiste en combinar y optimizar el uso de conceptos y tecnologías existentes como: Internet, granjas de ordenadores compartidos, gestión de recursos…etc[376]. También en el plano doctrinal Joyanes Aguilar subraya que "Desde un punto de vista práctico, la computación en nube, ha

---

[372]ARMBRUST, M., FOX, A., GRIFFITH, R., JOSEPH, A.D., KATZ, R.H., KONWINSKY, A., LEE, G.L, PATTERSON, D.A., RABKIN, A., STOICA, I. y ZAHARIA, M. Above the Clouds: A Berkeley View of Cloud computing. *Magazine Communications of the ACM*. April 2010. Vol. 53, Issue 4, p. 50-58 Disponible en web: http://www.cs.uoi.gr/~pitoura/courses/epl602/abovetheclouds.pdf

[373] Entrevista a Richard Stallman en The Guardian en fecha de 29 de septiembre de 2008. Disponible en web: https://www.theguardian.com/technology/2008/sep/29/cloud.computing.richard.stallman

[374] CRESPO PÉREZ, S., El Cloud Computing explicado [en línea]. *Telos. Cuadernos de Comunicación e Innovación*. 2009. Disponible en web: https://telos.fundaciontelefonica.com/url-direct/pdf-generator?tipoContenido=articulo&idContenido=2009111912530001

[375]FUNDACIÓN DE LA INNOVACIÓN BANKINTER, ob.cit, p. 27

[376] Resulta por cierto contradictorio con lo afirmado en este mismo documento en el párrafo inmediatamente anterior donde cataloga a la computación en nube como coherente con otras evoluciones, de igual magnitud, como el modelo cliente/servidor o Internet. ECONOMIC AND SOCIAL COMMITTEE OF THE EUROPEAN UNION. Cloud computing revolution - Why and how should Europe get ready? Disponible en web: http://www.eesc.europa.eu/?i=portal.en.ten-opinions.20566

venido a refundir conceptos ya extendidos de software como servicio, aplicaciones Web, cuya ejecución no requiere instalación ni mantenimiento, centros de datos y acceso a las aplicaciones desde cualquier lugar, cualquier dispositivo y en cualquier momento"[377].

Al margen de estas disquisiciones, la realidad es que estamos ante un paradigma evolutivo en las palabras de la ISO[378]. Más que una optimización, es una culminación de muchas de esas tecnologías, como por ejemplo el *grid computing*[379], el *utility computing*, SOA, Web 2.0 y otras tecnologías[380], de las cuales es necesario diferenciar[381] a la computación en nube. Efectivamente, como señalan Beltrán y Sevillano, "es necesario disponer de una tecnología como el Grid, que soporta las necesidades de recursos hardware que presenta, pero por otro también son necesarias tecnologías a un nivel de abstracción más alto….son la virtualización y los servicios web"[382].

Sin entrar en la definición y explicación de todos estos avances tecnológicos, sí que parece necesario detenerse siquiera sucintamente a explicar su diferenciación con respecto del *grid computing* ya que se caracterizan por compartir visiones similares: reducir costes de computación e incrementar la flexibilidad y la confiabilidad mediante el uso de hardware operado por terceros[383]. Para ello se pueden usar varios argumentos. Así, el propio origen de estas diferentes modalidades de computación ya que, como dice la Comisión Europea, mientras el *grid computing* trae causa de la investigación y posteriormente es exportado a la industria, en el caso del *cloud* el origen está directamente en los requerimientos y soluciones comerciales[384] por la estrecha conexión que existe entre tecnología y negocio[385]. Pero en

---

[377] JOYANES AGUILAR, La Computación en Nube (Cloud Computing): El nuevo paradigma tecnológico para empresas y organizaciones en la Sociedad del Conocimiento. *Icade. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales*. enero-abril 2009, nº 76, p. 95-111.

[378] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 17788. Information technology -- Cloud computing -- Overview and vocabulary

[379] KPMG describe el *grid computing* como la aplicación de los recursos de distintos ordenadores en una red a un único problema al mismo tiempo. KPMG , Modeling the economic impact of *cloud computing* [en línea], May, 2012, http://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Documents/modelling-economic-impact-*cloud*-computing.pdf

[380] *Opencloudmanifesto,* p. 2.

[381] La Comisión Europea se ha encargado de diferenciar el *cloud* de otros conceptos sin perjuicio de reconocer que estamos hablando de áreas muy relacionadas y que tienen un potencial impacto en el desarrollo futuro de la nube: la Internet de los Servicios, la Internet de las Cosas, el *grid computing* o las Arquitecturas orientadas al Servicio. EUROPEAN COMMISSION. Expert Group Report*, The Future of Cloud computing*. ob. cit., p. 16-18.

[382] BELTRÁN PARDO, M y SEVILLANO JAÉN, F. *Cloud Computing, tecnología y negocio*. Editorial Paraninfo. 2013. 167 p.

[383] VAQUERO, L.M., RODERO-MERINO, L., CÁCERRES, J. y LINDER, MAIK. Ob. Cit.

[384] EUROPEAN COMMISSION. Expert Group Report*, The Future of Cloud computing.* ob. cit., p. 5

[385] BELTRÁN PARDO, M y SEVILLANO JAÉN, F. ob. Cit. p. 6.

realidad existen también diferencias desde el punto de vista tecnológico, que son las relevantes a estos efectos y que quedan perfectamente reflejadas en el siguiente cuadro:

Parameter	Grid computing	Cloud computing
Goal	Collaborative sharing of resources	Use of service (eliminates the detail)
Computational focuses	Computationally intensive operations	Standard and high-level instances
Workflow management	In one physical node	In EC2 instance (Amazon EC2+S3)
Level of abstraction	Low (more details)	High (eliminate details)
Degree of scalability	Normal	High
Multitask	Yes	Yes
Transparency	Low	High
Time to run	Not real-time	Real-time services
Requests type	Few but large allocation	Lots of small allocation
Allocation unit	Job or task (small)	All shapes and sizes (wide & narrow)
Virtualization	Not a commodity	Vital
Portal accessible	Via a DNS system	Only using IP (no DNS registered)
Transmission	Suffered from internet delays	Was significantly fast
Security	Low (grid certificate service)	High (Virtualization)
Infrastructure	Low level command	High level services (SaaS)
Operating System	Any standard OS	A hypervisor (VM) on which multiple OSs run
Ownership	Multiple	Single
Interconnection network	Mostly internet with latency and low bandwidth	Dedicated, high-end with low latency and high bandwidth
Discovery	Centralized indexing and decentralized info services	Membership services
Service negotiation	SLA based	SLA based
User management	Decentralized and also Virtual Organization (VO)-based	Centralized or can be delegated to third party
Resource management	Distributed	Centralized/Distributed
Allocation/Scheduling	Decentralized	Both centralized/decentralized
Interoperability	Open grid forum standards	Web Services (SOAP and REST)
Failure management	Limited (often failed tasks/applications are restarted)	Strong (VMs can be easily migrated from one node to other)

Diferencias entre el *cloud y* el *grid computing*

Fuente: http://www.ipwithease.com/cloud-computing-vs-grid-computing/

Una vez hecha esta breve descripción de la evolución histórica de las tecnologías de computación, a día de hoy lo que podemos concluir es que la nube como recurso centralizado para la prestación integral de servicios a través de la Red sobre la base de la necesidad y la demanda de los usuarios supone dar a los usuarios, negocios, gobiernos y cualquier usuario la posibilidad de acceder a enormes recursos informáticos desde cualquier dispositivo y en cualquier lugar en que haya acceso a la red. Con independencia de que se trate de un

fenómeno evolutivo, de que se haya dado una convergencia de realidades tecnológicas ya existentes, de que se haya cerrado un círculo histórico, lo cierto es que estamos ante una tecnología que se ha ganado su sustantividad propia por la fuerza de los hechos. No se me ocurre una tecnología que no traiga causa de otra preexistente. La tecnología es evolutiva, aunque se hable de disruptiva, este sí es un concepto más "marketiniano" que tecnológico. La grandeza de esta evolución tecnológica, como hemos visto en el anterior capítulo, es que viene derivada de la convivencia y del intercambio. Basta recordar los famosos *Request for Comments* de la comunidad científica y académica. Aunque sea circular en el plano conceptual (de compartir a individualizar y vuelta a compartir, no pierde su dimensión evolutiva. Es puro darwinismo tecnológico: son las tecnologías que sobreviven las que sirven al desarrollo de otras. A ello se añade su dimensión finalista, el cloud ha conseguido acercar los recursos a cualquier consumidor sin importar el dispositivo con el que se acceda. Ha facilitado la vida al usuario. Si a ello le añadimos su dimensión de negocio, insistimos que sí se ha hecho merecedor de un reconocimiento individualizado sin el cual perdería cierto sentido este trabajo.

1.2 Modelos de servicio y modelos de implantación

El siguiente paso consiste en describir las características de los modelos de servicio y de los modelos de implantación que existen en la computación en nube. En primer lugar, se puede decir que existen fundamentalmente tres modelos de servicios o modelos de entrega de servicios que son prestados en nube y cuya nomenclatura se ha extendido de una manera generalizada en lo que se conoce como el "Modelo SPI"[386]: *Software as a Service*, *Infaestructure as a Service* y *Platform as a Service*. Bien es cierto que bajo la fórmula *X as a Service* se podría recoger cualquier otra modalidad. De hecho se habla también por ejemplo de *Process as a Service* (PraaS)[387] que se basa en la gestión externa y operada en Internet de un proceso de negocio de principio a fin, como puede ser la gestión delas reclamaciones,

[386] CLOUD SECURITY ALLIANCE. Guia para la Seguridad en áreas críticas de atención en *Cloud computing*. noviembre de 2009. Disponible en web: http://www.ismsforum.es/img/a25/na235_GUIA_CSA_PARA_LA_SEGURIDAD_EN_AREAS_CRITICAS_DE_ATENCION_EN_*CLOUD*_COMPUTING_V2.pdf, p. 7.

[387] FUNDACIÓN DE LA INNOVACIÓN BANKINTER y ACCENTURE. Ob. Cit. p. 41. Hay quienes lo denominan po su parte *Business Process as a Service* (BPaaS) y señalan que se encuentra en fase incipiente, siendo todavía un modelo de negocio en el que los proveedores tan solo operan en la actualidad en nichos concretos. OBSERVATORIO NACIONAL DE LAS TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN (ONTSI). *Cloud computing*. Retos y Oportunidades. Ministerio de Industria, Energía y Turismo. mayo 2012. Disponible en web: http://www.ontsi.red.es/ontsi/sites/default/files/1-_estudio_*cloud*_computing_retos_y_oportunidades_vdef.pdf,

de los gastos o de la cadena de suministro. Por ello, involucra no sólo a la organización, sino también a otros *stake holders*, como clientes y proveedores. Y lo más importante es que puede ser utilizado directamente por cualquier empleado, sin la intervención de profesionales de TI. O por ejemplo la ISO llega a hablar de hasta siete modelos de servicio diferentes, incluyendo *Network as a Service (NaaS)* y *Data Storage as a Service (DSaaS)*[388].

En todo caso, son los tres primeros los que gozan ya de una cierta tradición y que sin duda se encuentran genéricamente aceptados. Así, en el *SaaS* el consumidor utiliza una aplicación, pero no controla el sistema operativo, el *hardware* o la infraestructura de red en la que está ejecutando. Tiene como antecedentes a finales de la década de los noventa en las siglas ASP (*Application Service Provider*) con las que se definiría a los proveedores de servicios de aplicaciones, empresas que proporcionaban servicios de software a organizaciones desde un centro de computación y a través de una red, siendo Internet la más utilizada[389].

Sin lugar a dudas es la capa de la computación en nube que resulta más familiar a los usuarios individuales y no profesionales. Basta en este sentido pensar en el servicio que prestan la mayoría de los principales proveedores de servicios de correo electrónico (gmail, yahoo, Hotmail…), sin perjuicio de que existen multitud de aplicaciones enfocadas a la empresa (CRM por ejemplo). Se trata de un modelo de computación que es de gran utilidad tanto para los consumidores como para los prestadores del propio servicio en nube. Para los primeros como consecuencia de que pueden acceder al servicio "en cualquier momento y en cualquier lugar", compartir datos y colaborar más fácilmente, además de mantener sus datos almacenados de manera segura en la infraestructura; y para los segundos porque con una sola aplicación que mantener, los costes se reducen en comparación con el alojamiento de datos convencional.

En estos casos por tanto, el proveedor de servicios en nube instala, gestiona y mantiene el software. El proveedor no tiene por qué ser el propietario de la infraestructura en la que se ejecuta el software. El consumidor no tiene acceso a la infraestructura, solamente a la

[388] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 17788. Information technology -- Cloud computing -- Overview and vocabulary

[389] JOYANES AGUILAR, L. Computación en la nube e innovaciones tecnológicas. El nuevo paradigma de la Sociedad del Conocimiento [en línea]. *Grupo de Investigación de Ingeniera del Software y Sociedad de la Información y del Conocimiento*. Disponible en web: https://gissic.files.wordpress.com/2011/07/computacion_en_nube_revista_paraguay_luis_joyanes.pdf

aplicación. El ejemplo por excelencia en esta modalidad de servicio lo constituye la empresa Salesforce que como ya se ha apuntado, fue pionera en su prestación.

En cuanto al modelo *PaaS,* en él, el consumidor usa un entorno de almacenamiento para sus aplicaciones. El consumidor controla las aplicaciones que se ejecutan en el entorno (y posiblemente tiene algún control sobre el entorno de almacenamiento, pero no controla el sistema operativo, el *hardware* o la infraestructura de red en las que se está ejecutando). Al cliente se le proporciona un conjunto de herramientas y funcionalidades software (sistemas operativos y servicios asociados a los mismos) para desarrollo conjunto de software y aplicaciones situados en una red de máquinas accesibles a través de la red. Casos claros de éxito en este nivel del *cloud computing* son *Windows Azure Plattform* o *Google App Engine*. En estos casos por tanto, el proveedor de servicios gestiona la infraestructura de la nube para la aplicación, normalmente un marco para un tipo particular de aplicación. La aplicación del consumidor no puede acceder a la infraestructura por debajo de la plataforma. El modelo PaaS además, como dice Joyanes Aguilar, ha supuesto una verdadera democratización en el desarrollo de aplicaciones[390].

Por último, en el modelo *IaaS,* el consumidor usa "recursos fundamentales de la computación" tales como el poder de procesamiento, el almacenamiento, componentes de red (alquilando servidores, discos duros, procesamiento en un CPD…etc.). En este nivel de prestación de servicios, los proveedores son los propietarios de las máquinas y las ofrecen a los usuarios a través de entornos que les permiten gestionarlas. Uno de los claros casos de éxito respecto a la prestación de este tipo de servicios es *Amazon Web Services*. En estos casos el consumidor usa el servicio como si fuera una unidad de disco, base de datos…pero no tiene acceso a la infraestructura que lo almacena.

En definitiva como dice la Comisión Europea, el modelo SPI consiste en proveer una o más infraestructuras para plataformas, una plataforma para aplicaciones o unas aplicaciones en sí mismas vía servicios[391].

[390] JOYANES AGUILAR, L. Computación en la nube e innovaciones tecnológicas. El nuevo paradigma de la Sociedad del Conocimiento. Ob. Cit. p. 6

[391] EUROPEAN COMMISSION Expert Group Report, *The Future of Cloud computing. Opportunities for European Cloud computing Beyond 2010* ob. cit., p. 1

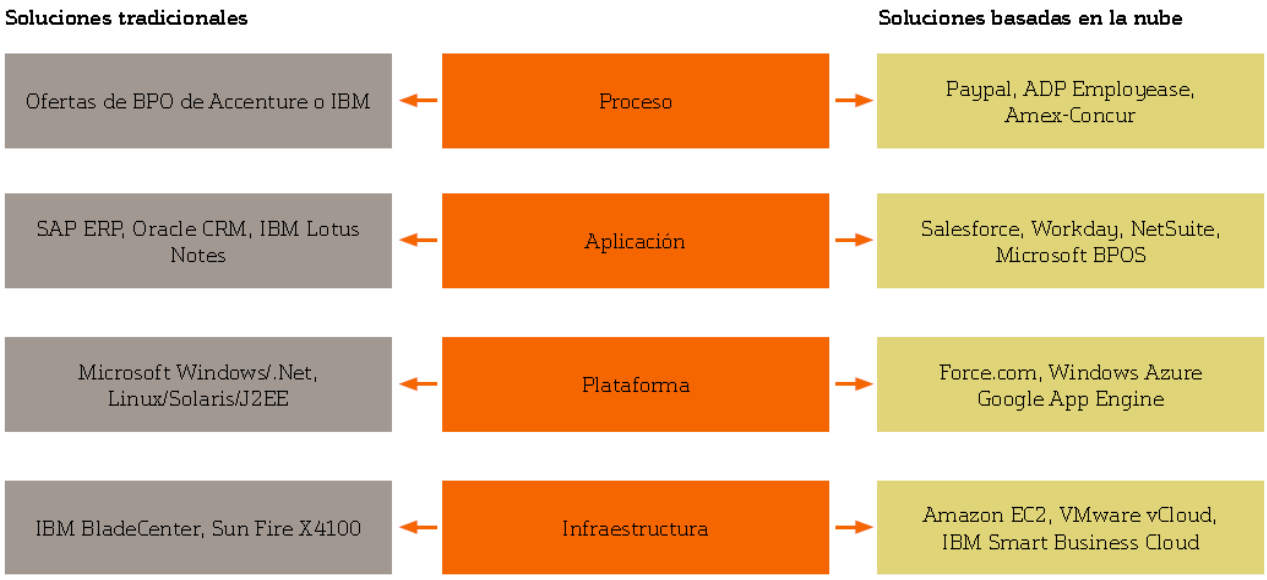
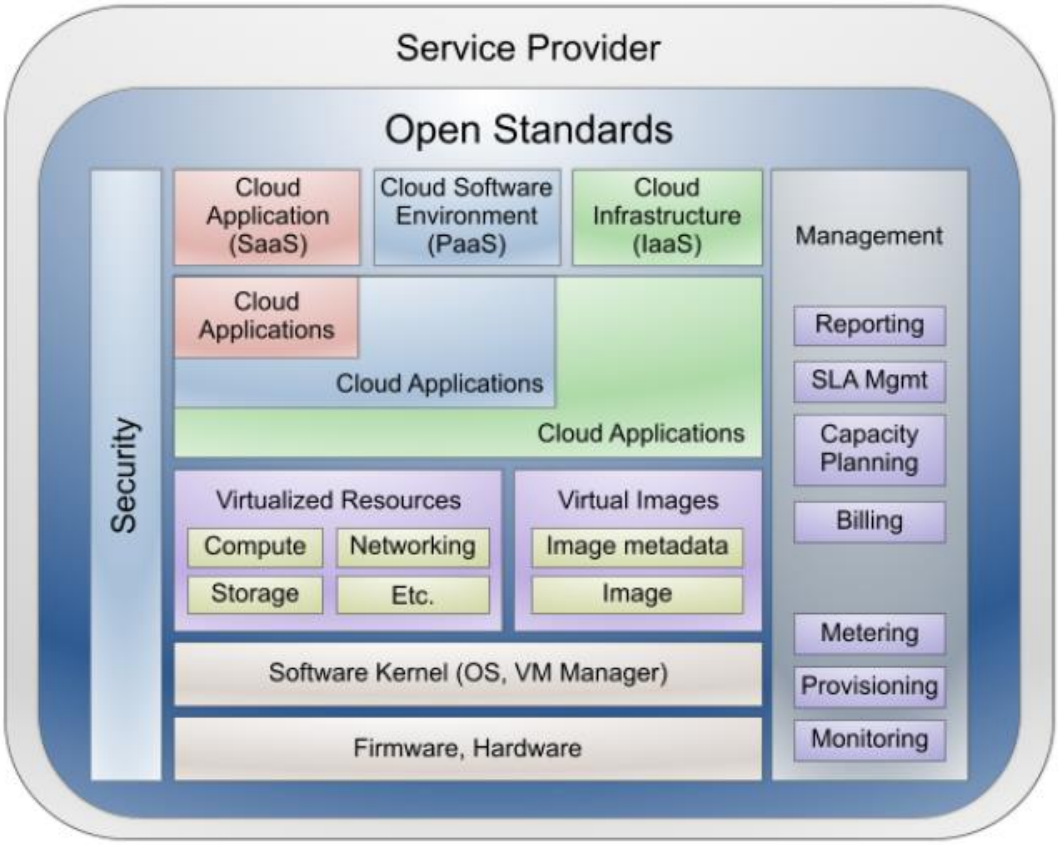


Ilustración 4: Soluciones tradicionales versus soluciones basadas en *cloud computing*.
Fuente: *What the Enterprise Needs to Know About Cloud computing*, Accenture (October 2009).

Fuente: Fundación Bankinter

A continuación reflejamos el diagrama de la computación en nube que hemos ido describiendo, desde el punto de vista del prestador del servicio, ya que desde el punto de vista del consumidor, dependiendo del tipo de prestación que busque, en determinadas ocasiones las interfaces que utilizan son como las de cualquier otra aplicación. La nube tiene como característica que la compleja estructura por debajo es ocultada al consumidor. Es lo que la Unión Europea ha denominado desmaterialización, esto es, los recursos informáticos son lo menos visibles posible para los usuarios ciudadanos o empresas[392]. En definitiva, como resume con sencillez Sosinsky, "la computación en la nube es una abstracción basada en la noción de reunir recursos físicos y presentarlos como un recurso virtual"[393].

[392] *Idem*
[393] SOSINSKY, B. *¿Qué es la nube? El futuro de los sistemas de información.* Anaya. 2012. 591 p.



Fuente: *Cloud computing Use Cases White Paper. Version 4.0*, 2010

Distinto es el caso, como decimos, del prestador de servicios[394]. En el referido diagrama la capa más baja es el firmware y el hardware en el que está basado todo lo demás y que conforman la "columna vertebral" de la nube[395]. Por encima de esto está el núcleo del software (*software kernel*), ya sea el sistema operativo o la máquina de gestión virtual que almacena la infraestructura bajo la nube. Los recursos virtualizados y las imágenes incluyen los servicios básicos de la computación en nube tales como el poder de procesamiento, el almacenamiento y el middleware. Las imágenes virtuales controladas por el gestor de la máquina virtual incluyen tanto las imágenes mismas como los metadatos, que no dejan de

[394] CLOUD COMPUTING USE CASE DISCUSSION GROUP. Cloud compunting Use Cases White Paper. Version 4.0. 2 de julio de 2010. Disponible en web: http://open*cloud*manifesto.org/*Cloud*_Computing_Use_Cases_Whitepaper-4_0.pdf

[395] YOUSEFF, L., BUTRICO, M., y DA SILVA, D. Toward a Unified Ontology of Cloud Computing. *Grid Computing Environments Workshop*. 2008. Disponible en web: https://pdfs.semanticscholar.org/3d9c/9982b639be42e97c1d0dc4b5ce74d163f064.pdf
Aunque en puridad las citadas autoras hablan del hardware físico y los interruptores como los que conforman la citada columna vertebral.

ser datos que describen otros datos, necesarios para gestionarlas. Y es ya a partir de esas capas cuando se comienza a prestar el servicio bajo alguno de los modelos antes citados[396].

Una característica propia de esta arquitectura es que, como señala el NIST, los elementos físicos del entorno de la nube, con independencia del modelo de servicio ante el que estemos, son siempre controlados por el proveedor de servicios. Nos estamos refiriendo a la calefacción, la ventilación, el aire acondicionado [los tres son conocidos genéricamente por el acrónimo inglés (HVAC)], la potencia, las comunicaciones y otros aspectos de la planta física que componen la última de las capas; y también a los ordenadores, la red y los componentes de almacenamiento, así como otros elementos físicos que componen el *hardware*[397].

Otro elemento relevante para el proveedor es el concerniente a la gestión de las capas. En el nivel más bajo, la gestión requiere medidas para determinar quién usa el servicio y en qué medida, haciendo las provisiones para determinar cómo los recursos son asignados a los consumidores, y controlados para realizar un seguimiento del estado del sistema y de sus recursos. En el nivel más alto por su parte, la gestión incluye la facturación para recuperar los costes, la capacidad de planificación para asegurar que las demandas del consumidor se satisfacen, y la gestión en definitiva de los acuerdos de nivel de servicio (SLA) para asegurar que los términos de servicios acordados por el prestador y el consumidor se respetan.

Además de los modelos de servicio a los que nos acabamos de referir, ya hemos adelantado que se ha generalizado igualmente la existencia de diferentes modelos de nubes o, de manera más correcta, distintas modalidades de implantación o modelos de despliegue de este servicio. En concreto se habla de cuatro tipos: nubes públicas, nubes comunitarias, nubes privadas y nubes híbridas[398].

---

[396] No obstante cabe decir que en determinadas ocasiones hay un uso de esta capa de la nube por parte de grandes empresas con gigantescos requerimientos de tecnologías de la información que necesitan subarrendar *Hardware as a Service* (HaaS). *Idem*, p. 6.

[397] JANSEN, W. y GRANCE, T., Guidelines on Security and Privacy in Public Cloud computing. *National institute of Standards and Technology* (*NIST*), *U.S. Department of Commerce.* Diciembre de 2011. Disponible en web: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

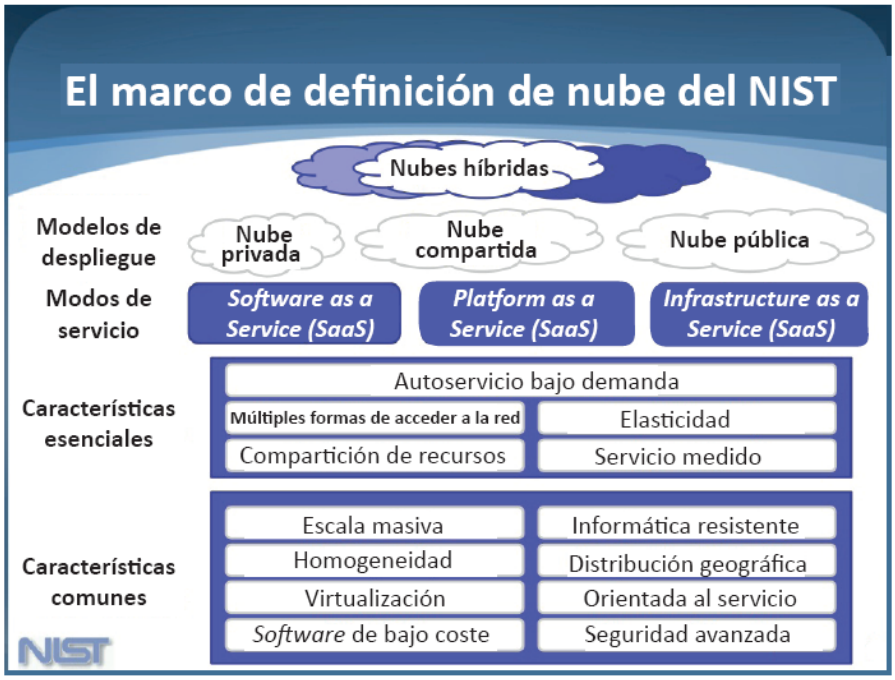
[398] Es la clasificación más generalizada que se encuentra recogida en cualquiera de los documentos citados referidos a la nube en general. La Comisión Europea ha hablado sin embargo también de "Nubes de finalidad específica" (*Special Purpose Clouds*) que define como extensiones de sistemas de nube "normales" para proveer capacidades adicionales. EUROPEAN COMMISSION. Expert Group Report, *The Future of Cloud computing. Opportunities for European Cloud computing Beyond 2010* ob. cit., p. 11. Por su parte también hay quienes hablan de "Nube gestionada" que se caracterizaría por estar dedicada a una o varias entidades usuarias, estando gestionada por un proveedor externo y estando albergada en infraestructuras de uno de sus usuarios (nube gestionada para este usuario, para el resto de usuarios sería una nube pública).

- **Nubes privadas:** la infraestructura de la nube es operada solamente para una organización. Puede ser gestionada por la organización o por un tercero y puede existir en las instalaciones o fuera de las instalaciones.
- **Nubes comunitarias**[399]**:** la infraestructura de la nube es compartida por varias organizaciones y presta soporte a una comunidad específica que ha compartido preocupaciones (objetivos, requisitos de seguridad, políticas y consideraciones relativas al cumplimiento). Puede ser gestionado por las organizaciones o terceras partes y puede existir fuera o dentro de las instalaciones.
- **Nubes públicas:** La infraestructura de la nube es puesta a disposición del público en general o de un amplio grupo empresarial y es propiedad de una organización que presta servicios en nube.
- **Nube híbrida:** La infraestructura de la nube es una combinación de dos o más nubes (privadas, comunitarias o públicas) que son entidades únicas pero están unidas a través de una tecnología estandarizada que permite la portabilidad de datos y aplicaciones (por ejemplo para equilibrar la carga entre las nubes).

El resumen de todo lo expuesto se encuentra plasmado en la siguiente figura

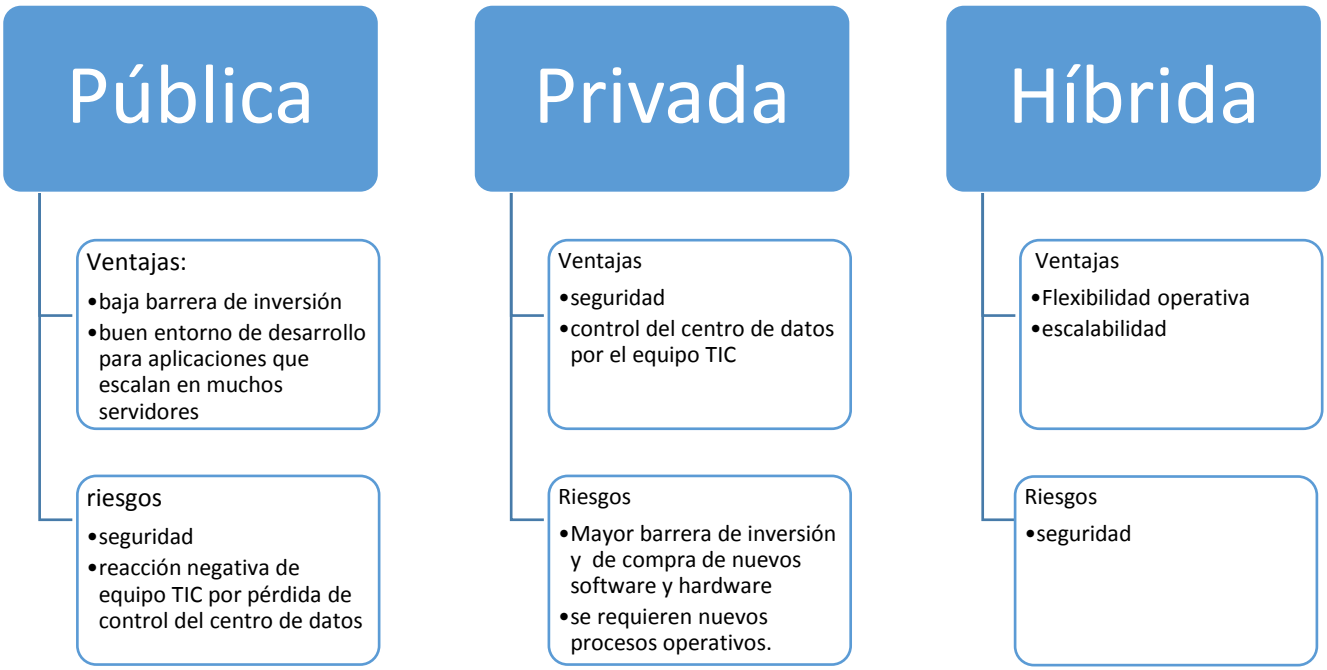
AREITIO, J. Protección del *Cloud computing* en seguridad y privacidad. *REE.* mayo de 2010. p. 42. Disponible en web: http://www.redeweb.com/_txt/666/42.pdf
A esta clasificación cabría añadir otra que está menos generalizada y que distingue entre nube interna y nube externa, caracterizándose la primera por estar situada en el centro de procesamiento de datos de la empresa y formar parte de los activos capitalizados por ésta; y la segunda por estar alojada fuera del entorno de la empresa y formar parte de los activos del proveedor de servicio. Fundación Bankinter, ob.. cit., p. 90.

[399] Hay quienes consideran que las nubes comunitarias no son sino una subdivisión de las nubes privadas. JOYANES AGUILAR, L. Computación en la nube e innovaciones tecnológicas. El nuevo paradigma de la Sociedad del Conocimiento. ob. cit., p. 7.



Fuente: NIST, 2011

La decisión sobre el modelo de implantación por parte de una organización va a estar sometido a un conjunto de factores, por cuanto cada uno de ellos, como refleja la siguiente figura, tiene sus ventajas y sus inconvenientes y consiguientemente dependerá del peso que la organización correspondiente otorgue a cada uno de ellos:



Fuente: elaboración propia con base en la Guía elaborada por *SearchCloudcomputing.com*[400]

2 La proyección económica del *cloud computing*.

La segunda de las perspectivas de análisis de la computación en nube, es la relativa a su proyección económica o su impacto de negocio y en los negocios. Se trata de una perspectiva particularmente relevante incluso como elemento diferenciador. Ya se ha apuntado más arriba la importancia de esta conexión como uno de los factores para distinguirlo del *Grid computing* y es que mientras esta está fundamentalmente apoyada por el gobierno y la academia y la generación de beneficio no es suficientemente importante, el *cloud* está apoyado por las grandes empresas tecnológicas[401]. Además, desde la perspectiva de la utilidad pública que tanto se ha subrayado, pocos son los casos en los que, como en el *cloud*, nos encontramos con tantos servicios "gratuitos"[402], aunque sin duda esta última

[400] SEARCHCLOUDCOMPUTING.COM. E-guide. Differences explained: Private vs. public vs. hybrid cloud computing. Sponsored by HP and Intel. Disponible en web: http://docs.media.bitpipe.com/io_10x/io_100433/item_419065/HPIntel_sCloudComputing_SO%23034437_E-Guide_052611.pdf
[401] GONG, C., LIU, J., ZHANG, Q, CHEN, H, y GONG, Z. The Characteristics of Cloud Computing. *39th International Conference on Parallel Processing Workshops*. 2010. P. 275-279
[402] *Ídem*. p. 278.

palabra no es del todo cierta si se tienen en cuenta, desde la teoría del consumidor, que el consumidor ya hace "micropagos" a los proveedores facilitando información personal en lo que se ha venido en denominar la "economía de la privacidad"[403].

Algunos de los estudios más recientes nos permiten dar cifras que arrojan algo de luz sobre la dimensión de negocio de esta tecnología. Sin ánimo de ser exhaustivos, se puede señalar algunos datos[404]: Morgan Stanley prevé que los productos *cloud* de Microsoft (Office365, CRM, and Azure) producirán un 30% de los ingresos en 2018, frente al 11% que supusieron en 2015; en 2015 Amazon Web Services (AWS) generó un 69% más de ingresos que en 2014; el gasto mundial en servicios *cloud* públicos está previsto que pase de cerca de 70.000 millones de dólares en 2015 a superar los 141.000 en 2019. Este último dato supone que el índice de crecimiento de los servicios de *cloud computing* será seis veces la media del crecimiento de gasto en todo el sector TIC[405].

En un ámbito geográfico más limitado, la Unión Europea ha señalado que Europa posee importantes ventajas para resultar competitivo desde el punto de vista económico en el mercado del *cloud computing*[406]:

Infraestructura digital	La fibra óptica tiene un amplio desarrollo
CPP o PPP *(public private parnership)*	Europa sabe usar la política de inversión pública como catalizadora de la inversión privada
Estructura de PYMES	Las PYMES buscan interlocutores de proximidad
Determinados sectores	Las restricciones normativas de determinados sectores conllevan proveedores nacionales o europeos.

[403] BAYRAK, E., CONLEY, J.P., WILKIE, S. The Economics of Cloud Computing. *The Korean Economic Review*. September 2009. Vol., nº 27, p. 203-220.
[404] COLUMBUS, L., Roundup of Cloud Computing Forecasts and Market Estimates, 2016. *Forbes*. 13 de marzo de 2016. Disponible en web: http://www.forbes.com/sites/louiscolumbus/2016/03/13/roundup-of-cloud-computing-forecasts-and-market-estimates-2016/#222be86274b0
[405] INTERNATIONAL DATA CORPORATION. Worldwide Semiannual Public Cloud Services Spending Guide. 2016. Disponible en web: http://www.idc.com/getdoc.jsp?containerId=IDC_P33214
[406] ECONOMIC AND SOCIAL COMMITTEE OF THE EUROPEAN UNION. Cloud computing revolution - Why and how should Europe get ready? Ob. Cit.

Fuente: elaboración propia

En concreto la Comisión Europea ha dicho que el *cloud computing* va a jugar un papel preponderante del sector TIC en los próximos diez años o más y ello fundamentalmente por las siguientes razones[407]: cada vez más empresas buscan externalizar sus tecnologías de la información, algunos negocios requieren de capacidad adicional temporalmente para necesidades particulares, se pueden explotar los sistemas de nube con fines experimentales evitando así alteraciones, cabe utilizar el servicio *cloud* como un territorio neutral para operaciones empresariales conjuntas, favorece la continuidad del negocio y la recuperación en caso de desastre, provee un punto de entrada de bajo coste en la provisión de tecnologías de la información y de la comunicación para una empresa.

Desde el sector privado, la prestigiosa consultora Gartner señalaba a finales de 2009 que el *cloud computing* iba a ocupar el primer puesto en el área tecnológica estratégica para el año 2010. En una encuesta que la propia consultora realizó a cerca de dos mil CIO's del sector se ponía igualmente de manifiesto que el *cloud computing* era una de las prioridades tecnológicas de 2011. En el caso concreto de España por ejemplo, puede ser una tierra fértil para el desarrollo de esta tecnología, en gran medida porque el 43 % de los trabajos están en el sector servicios que es el área mejor posicionada para liderar la migración a la nube[408]. Como dice Irving Wladawsky-Berger, presidente emérito de la Academia de Tecnología de IBM y experto del *Future Trends Forum*, la aparición del *cloud computing* marca un hito de vital importancia en la aplicación de las TIC a la mejora del sector servicios, base principal de las economías modernas[409].

A la perspectiva del sector beneficiario, también cabría añadir la perspectiva del tamaño de las empresas, que resulta de particular interés por ser el foco de nuestro trabajo. En el caso de nuestro país hay que destacar el especial impacto beneficioso que tiene para las PYMES, que constituyen una parte muy importante en la estructura económica española[410]. Aunque lo cierto es que también para las grandes empresas puede suponer un ahorro económico fundamentalmente mediante la conversión de determinados costes fijos en costes

[407] EUROPEAN COMMISSION Expert Group Report, *The Future of Cloud computing. Opportunities for European Cloud computing Beyond 2010*. ob. cit. p. 44.
[408] Spain is Ripe for Cloud computing but Slow to Adopt. *New York Times.* September 19th, 2010.
[409] FUNDACIÓN DE LA INNOVACIÓN BANKINTER. ob. Cit. p. 32
[410] OBSERVATORIO SAGE. Radiografía SAGE de la PYME en España 2015. En el 2015 las pymes representan el 99,88% de las empresas españolas.

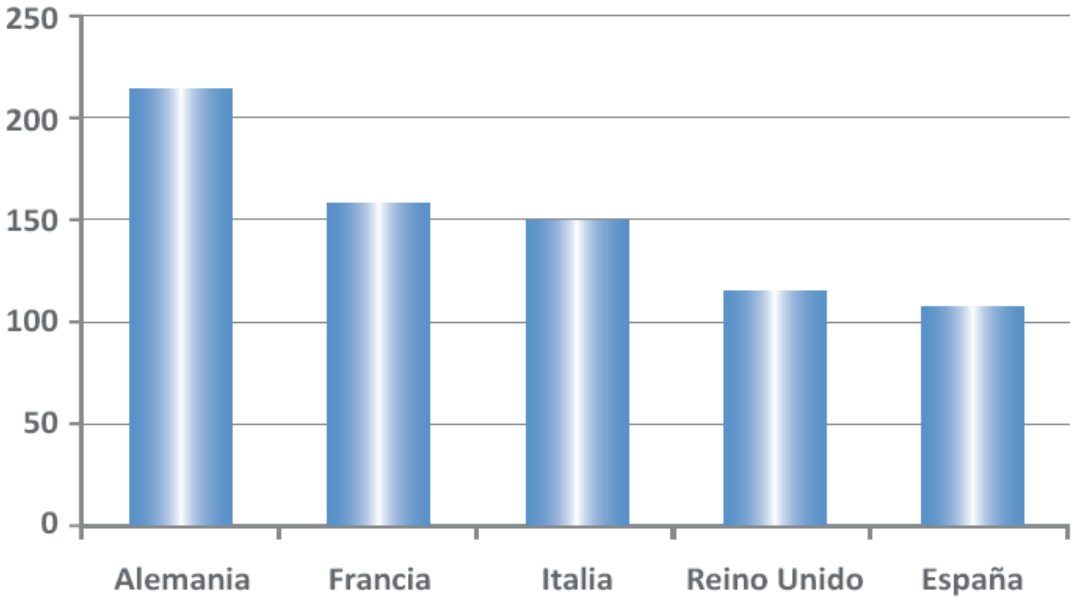
variables[411]. Ciertamente, con independencia del tamaño, las nuevas empresas que, por principio, están en una fase de desarrollo expansivo, tienen en la computación en nube una herramienta vital para una rápida adaptación de sus necesidades de computación al crecimiento del negocio[412].

La perspectiva de negocio se puede analizar desde el punto de vista macroeconómico o microeconómico[413]. Al igual que cualquier otra innovación tecnológica, la computación en nube también proyecta sus beneficios en el plano macroeconómico, máxime en el marco de una economía totalmente globalizada. La OCDE subraya que desde el punto de vista macroeconómico, el estudio se tiene que focalizar en dos aspectos: la potencial reducción de costes por parte del usuario, y el impacto de esta tecnología en el crecimiento del PIB y su impacto en la creación de empleos, particularmente en el sector privado [414]. Adicionalmente habría que añadir, de nuevo, otro tipo de costes de más difícil medición, como los derivados del ahorro energético provocado por el uso más eficiente de la infraestructura de las TIC que esta nueva tecnología permite[415]. A título de ejemplo, como demostró el estudio elaborado por la Agencia de Protección Medioambiental de Estados Unidos, solo la virtualización puede ofrecer un significativo ahorro de energía para los servidores de volúmenes porque estos servidores funcionan habitualmente a una media de nivel de utilización de procesamiento de entre tan solo el 5% y el 15%[416]. Especialmente interesante, cabría añadir, para países con una fuerte dependencia energética como es el caso de España.

En el plano doctrinal, desde el punto de vista macroeconómico y en lo referido al impacto sobre el PIB sigue siendo referencia, a pesar de que ya tiene una cierta antigüedad, el estudio

[411] FUNDACIÓN DE LA INNOVACIÓN BANKINTER ob. cit., p. 7. No obstante parecen ser más reticentes a la hora de observar los beneficios derivados de esta tecnología. *Idem*. p. 70 y ss.
[412] ECONOMIC AND SOCIAL COMMITTEE OF THE EUROPEAN UNION. Cloud computing revolution - Why and how should Europe get ready? Ob. Cit.
[413] Ambas perspectivas se encuentran incluidas en el informe elaborado por el CENTER FOR ECONOMICS AND BUSINESS RESEARCH. *THE CLOUD DIVIDEND: Part One The economic benefits of cloud computing to business and the wider EMEA economy France, Germany, Italy, Spain and the UK*. December 2010. Disponible en web: https://uk.emc.com/collateral/microsites/2010/cloud-dividend/cloud-dividend-report.pdf
[414] OECD. Cloud Computing: The Concept, Impacts and the Role of Government Policy. Ob. Cit. p. 13.
[415] CIERCO, D (Coord.). *Cloud computing: retos y oportunidades*. Fundación Ideas. 2011. http://www.fundacionideas.es/sites/default/files/pdf/DT-*Cloud*_Computing-Ec.pdf, páginas 20 y 21.
[416] US ENVIRONMENTAL PROTECTION AGENCY. ENERGY STAR PROGRAM. Report to Congress on Server and Data Center Energy Efficiency. Public Law 109-431. August 2, 2007. Disponible en web: https://www.energystar.gov/sites/default/files/buildings/tools/Report%20to%20Congress%20on%20Server%20and%20Data%20Center%20Energy%20Efficiency.pdf

elaborado por el profesor Etro[417], quien proyectaba, en el ámbito circunscrito a la UE, un crecimiento en el PIB a corto plazo entre el 0,05% y el 0,15% y a medio plazo entre el 0,1% y el 0,3%, estando condicionado el margen en función de la velocidad en la implantación de esta tecnología. También el *Center for economics and Business research* en su informe de 2010 presentaba el siguiente gráfico sobre el potencial de ganancias acumuladas hasta el año 2015 derivadas del *cloud computing* en las principales economías europeas:



Fuente: *Center for economics and Business research*, 2010.

El efecto dinamizador, según el ONTSI deriva del hecho de que los beneficios que obtienen las empresas prestadoras de *cloud* se reinvierte en la economía por la vía de consumos intermedios en otros sectores derivados, genera una dinamización del empleo cualificado e incrementa el poder adquisitivo y el consumo en un territorio[418]:

Por cada euro invertido en *cloud* ⟹ impacto positivo superior en el PIB

[417] ETRO, F. The Economic Impact of Cloud Computing on Business Creation, Employment and Output in the E.U. An application of the Endogenous Market Structures Approach to a GPT innovation. *Review of Business and Economics*. 2009, 54(2), p. 179-208.
[418] ECONOMIC AND SOCIAL COMMITTEE OF THE EUROPEAN UNION. Cloud computing revolution - Why and how should Europe get ready? Ob. Cit.

Más allá de lo numérico, pero también en el plano macroeconómico, los efectos principales son[419]: menores barreras de entrada y efectos en la innovación; potencial para incrementar la producción y el empleo en industrias no tecnológicas, en lo que se conoce como efectos de gasto secundarios; potencial para bajar precios, aumento e inflación en el largo plazo; y por último, la utilización por el sector público puede reducir el gasto gubernamental. En referencia a este último efecto, y con base en la investigación llevada a cabo por West en 2010 tras analizar diversos casos de agencias norteamericanas que habían dado el salto a la nube, el potencial de ahorro de costes en los gobiernos se mueve entre el 25 y el 50%[420].

Es necesario completar la visión macroeconómica con una vertiente que muchas veces se olvida en este tipo de análisis y que sin embargo es también fuente de competitividad y de generación de negocio. Efectivamente, además de esta perspectiva que ha ido enfocada a los potenciales usuarios empresariales (grandes empresas o pymes), también hay que observar los beneficios económicos para las empresas que facilitan el entorno de la computación en nube, las empresas del sector tecnológico. Siguiendo el Dictamen publicado a principios de 2012 por el Consejo Económico y Social de la Unión Europea, podemos señalar las siguientes[421]:

Empresas integradoras de sistemas	Editores de programas informáticos	Empresas de alojamiento de sistemas
Se seguirán encargando del diseño y desarrollo de los servicios de computación en nube	Deben realizar enormes inversiones en la reconversión de los productos puesto que la nube pone en entredicho determinados modelos de negocio (*cloud computing ready*)	La nube refuerza enormemente al sector favoreciendo la competitividad entre los proveedores

[419] PACKY LAVERTY, J., WOOD, D.F., y TURCHEK, J. Micro and Macro Economic Analysis of Cloud Computing. *Issues in Information Systems*, 2014. Vol. 15, Issue II, p. 293-302.
[420] WEST, P. Saving Money Through Cloud Computing. *Governance Studies*. The Brookings Institutions, Washington. 2010. Disponible en web: https://www.brookings.edu/wp-content/uploads/2016/06/0407_cloud_computing_west.pdf
[421] ECONOMIC AND SOCIAL COMMITTEE OF THE EUROPEAN UNION. Cloud computing revolution - Why and how should Europe get ready? Ob. Cit.

Fuente: elaboración propia[422]

Desde el punto de vista microeconómico, este tipo de tecnología presenta numerosas ventajas. En primer lugar, y quizá como beneficio más destacable, las economías de escala, consecuencia de que los operadores de los servicios de *cloud computing* prestan numerosos servicios estandarizados a muchos clientes, lo que proyecta en éstos un aumento de su productividad. Precisamente desde la perspectiva de los clientes es desde donde se observan, siguiendo a José Antonio Fernández[423], las principales ventajas de esta nueva tecnología:

- Permite el acceso inmediato a los servicios ofrecidos por el operador sin haber tenido que adquirir previamente el hardware y el software necesarios y construir, instalar y gestionar los sistemas por sí mismos.
- Evita la inversión financiera inicial asociada al punto anterior, y a cambio los clientes pagan por el uso que realicen de los servicios, reduciéndose también las inversiones fijas en TIC[424]. En definitiva, ya no existe la denominada barrera de entrada, lo cual favorece la competitividad. Se puede decir que las empresas puede competir en igualdad de condiciones en el área de las tecnologías con cualquier empresa de cualquier tamaño. La ventaja competitiva ya no está en quién tiene los recursos de cómputo, sino en quien los emplea mejor[425]. Es lo que desde el punto de vista financiero en definitiva se denomina una conversión de CAPEX a OPEX, o de fijo a variable. Además el sistema *cloud* favorece posteriormente, debido al modelo *pay as you go*, el cumplimiento de los requerimientos internos y externos en las auditorías de las empresas.
- Costes anuales totales potencialmente inferiores debido a las economías de escala de los grandes *datacenters* que atienden a muchos usuarios. Además, como señala

[422] La Unión Europea ha señalado la necesidad de agrupar a los editores de servicios de computación en nube y a las empresas de telecomunicaciones, dado que estos últimos están por naturaleza en contacto directo con los usuarios interesados en dichos servicios. *Idem.*
[423] FERNÁNDEZ, J.A. *Cloud computing*: ¡un futuro brillante! *NOTA ENTER. Instituto de Empresa*. nº 122. 17 de marzo de 2009. Disponible en web: https://observatorio.iti.upv.es/media/managed_files/2009/03/23/10550.pdf
[424] ONTSI, ob. cit., pp. 26 y 27.
[425] ECHEVERRI GARCÍA, E. El futuro está aquí: computación en nube. *Revista Sistemas*. 2008, nº. 108. p. 53-56.

el mencionado estudio de la empresa IBM[426], la nube ofrece algo más que escalabilidad en las tecnologías de la información, puesto que facilita a la organización la posibilidad de que esa escalabilidad se proyecte hacia las operaciones de negocio[427]. Lo mismo cabe decir respecto de las medidas de seguridad, puesto que todas las medidas adoptadas al respecto serán más baratas si se implantan a gran escala[428]. Es fundamental en todo caso llevar a cabo un análisis con la finalidad de sopesar si se cumplirá el objetivo del retorno de la inversión poniendo en un lado de la balanza los recursos externalizados (se entiende a una nube pública) frente al incremento de la infraestructura local y el uso de tecnologías de nube privada[429].

- Aplicaciones disponibles desde cualquier punto con acceso a Internet e integración más simple con clientes y proveedores permitiendo trabajar con ellos de forma más fácil e interactiva. Dentro de este mismo punto añade la Unión Europea ventajas de tipo laboral, puesto que esa nota característica favorece la movilidad de los asalariados en el marco de la organización interna de la empresa[430]; así como también, de manera inevitable, como recuerda el Observatorio nacional de las telecomunicaciones y la Sociedad de la Información (en adelante ONTSI), el ahorro en recursos humanos al no necesitar un departamento de TIC que puede ser reducido considerablemente[431].
- Mayor facilidad de absorber picos de carga y de ampliar la capacidad de proceso.
- Garantía ante desastres. Una red de grandes *datacenters* debe ser capaz de ofrecer garantía de continuidad de servicio en caso de desastre con mayores garantías y menores costes (aunque a fecha de hoy no todos los operadores lo ofrezcan).

Estos análisis de las ventajas desde el punto de vista económico y, más concretamente, desde el punto de vista financiero, se han generalizado, con más o menos matices. Así, a título de ejemplo, desde la Universidad de Berkeley se señala que, desde el más concreto

[426] IBM INSTITUTE FOR BUSINESS VALUE. The power of cloud. Driving business model innovation. ob. cit., p. 5.
[427] ENISA. Cloud computing: Benefits, risks and recommendations for information security. Noviembre 2009. 125 p. Disponible en web: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/*cloud*-computing-risk-assessment/
[428] *Idem*. p. 17.
[429] EUROPEAN COMMISSION. Expert Group Report. ob. cit. p. 14.
[430] ECONOMIC AND SOCIAL COMMITTEE OF THE EUROPEAN UNION. Cloud computing revolution - Why and how should Europe get ready? Ob. Cit.
[431] ONTSI, ob. cit., p. 26 y 27.

punto de vista del hardware, el *cloud computing* conlleva tres nuevos aspectos[432]: la ilusión de disponibilidad bajo de demanda de una infinidad de recursos de computación, la eliminación de la barrera de entrada para los usuarios del *cloud*, y la posibilidad de pagar por el uso de recursos de computación en un corto plazo en función de las necesidades[433].

A las ventajas anteriormente mencionadas, se añaden otras que si bien no son estrictamente una característica propia del *cloud* tienen sin embargo una indudable repercusión[434]. Esto se puede señalar de lo que se conoce como el factor "verde", es decir, el hecho de que se produce un fuerte ahorro en energía, dado que el consumo energético es más eficiente en los centros de procesamiento y almacenamiento compartidos frente a los individuales de las empresas [435]. Igualmente supone también una reducción de la emisión de gases contaminantes [436] y de lo que se conoce como "la huella del carbono" [437]. Idéntico razonamiento realiza ONTSI al recordar que los principales factores que permiten reducir el consumo de energía y la emisión de gases son el aprovisionamiento dinámico, la naturaleza multi-arrendataria[438], la utilización de servidores y la eficiencia del centro de datos.

Merece en este punto destacarse una de las infraestructuras esenciales para la tecnología *cloud*: los *datacenters* o megacentros de datos construidos por los principales proveedores de servicios en nube. Estas empresas son algunos de los grandes consumidores de energía y por ello han desarrollado sus centros de datos como proyectos verdes de tal modo que cumplan las siguientes condiciones[439]: tener acceso a energía de bajo coste, beneficiarse de una fuente de energía renovable y estar cerca de agua abundante. Efectivamente, "las empresas prestadoras de los servicios asociados a la Cloud Computing los han desarrollado como "proyectos verdes" que reúnen condiciones ecológicas y sostenibles: con energías

---

[432] ARMBRUST, M., FOX, A., GRIFFITH, R., JOSEPH, A.D., KATZ, R.H., KONWINSKY, A., LEE, G.L, PATTERSON, D.A., RABKIN, A., STOICA, I. y ZAHARIA, M. Above the Clouds: A Berkeley View of Cloud computing. *Magazine Communications of the ACM*. April 2010. Vol. 53, Issue 4, p. 50-58 Disponible en web: http://www.cs.uoi.gr/~pitoura/courses/epl602/abovetheclouds.pdf

[433] Pensemos por ejemplo en el sistema *Stop Instancies* de Amazon que configura un sistema de acceso a los excedentes de almacenamiento de la compañía muy similar al establecido para la energía sobrante.

[434] Se calcula que Internet consume aproximadamente el 10 por 100 de la energía total del mundo. SOSINSKY, B. ob. Cit. p. 41.

[435] FUNDACIÓN DE LA INNOVACIÓN BANKINTER. ob. cit., p. 32.

[436] ONTSI. ob. cit. p. 29.

[437] EUROPEAN COMMISSION. Expert Group Report. ob. cit. p. 14.

[438] Para profundizar en particular en esta interesante faceta del *cloud*, ver ALJAHDALI, H., ALBATI, A., GARRAGHAN, P., TOWNEND, P., LAU, L., y XU, J. Multi-tenancy in Cloud Computing. *8th IEEE International Symposium on Service Oriented System Engineering. SOSE 2014*. Oxford. United Kingdom, April 7-11, 2014. IEEE Computer Society 2014. p. 344-351.

[439] SOSINSKY, B. ob. cit., p. 40.

renovables, con impactos menores en el entorno, aprovechando accesos ya existentes a las redes principales de alta velocidad, etc."[440]

De la cadena de valor hasta ahora apuntada que aporta el *cloud computing*, la perspectiva de reducción de coste es la más comúnmente analizada, fundamentalmente como consecuencia de que es la más fácil de medir. No obstante, debe ser completada por la perspectiva que da el aumento del beneficio: la escalabilidad, el autoservicio bajo demanda y el pago por uso favorecen la competitividad frente al modelo tradicional. Y es que existen claros beneficios derivados no tanto de la reducción de costes como del aumento de la productividad, incrementando el *output* derivado de cada unidad de coste. Hay que tener en cuenta que los cambios en los negocios pueden conseguirse sin necesidad de un planeamiento de capacidades detallado ni cambios en la tecnología instalada, ni la adquisición de nueva tecnología[441]. Desde el punto de vista de su proyección de negocio pensemos también en la posibilidad de abrir oficinas, trasladar personal (movilidad laboral antes citada) y operaciones geográficamente sin necesidad de comprometer el acceso a los sistemas de negocio[442].

A pesar de todas las ventajas económicas que acabamos de señalar, no todos los datos respecto de la adopción de la tecnología *cloud* son tan satisfactorios. Según la última encuesta llevada a cabo por Eurostat en 2014 específicamente sobre el ámbito del *cloud computing*, podemos observar cómo solamente el 19 % de las empresas europeas utilizaron este tipo de tecnología, la mayoría para el almacenamiento de sus sistemas de correo y el archivo de expedientes en formato electrónico; el 46% de dichas empresas utilizaron servicios más avanzados relativos a aplicaciones financieras y de contabilidad, CRMs o utilizaron el poder de computación para la ejecución de aplicaciones de negocio; en 2014 casi el doble de empresas utilizaron servidores de nubes públicas (12 %) que privadas (7 %); mientras que cuatro de cada die empresas (39 %) que utilizan esta tecnología informaron que el riesgo de quiebras en la seguridad es el principal factor de limitación a la hora de utilizar estos servicios; y similar era la proporción (42%) de los que alegaban que era el insuficiente conocimiento de esta tecnología como principal motivo para no utilizarla[443]. Y es

[440] CABARCAS ÁLVAREZ, A., PUELLO MARRUGO, P. y CANABAL MESTRY, R. *Cloud Computing:* tecnología verde como estrategia para la responsabilidad social empresarial. *Saber, Ciencia y Libertad*. 2012, vol. 7, nº 2, p. 135-142.
[441] KPMG. ob. cit. p. 9
[442] *Idem*, p. 21.
[443] GIANNAKOURIS, K. y SMIHILY, M. Cloud computing - statistics on the use by enterprises. *Eurostat.* November 2014. Disponible en web: http://ec.europa.eu/eurostat/statistics-

que, como vamos a ver, y aquí radica la fundamentación de nuestro estudio, el *cloud computing* disponiendo de muchas ventajas, también asume muchos retos.

3 Retos del cloud computing[444].

Es preferible hablar de retos, si, como señala el NIST, consideramos que a este concepto se llega si se dan los pasos para reducir el riesgo a un nivel aceptable[445].

Como afirma *Cloud Security Alliance* el problema principal del *cloud*, y en el que podrían resumirse los principales riesgos que afronta, radica en la gestión del ciclo de vida de la información que afecta a la seguridad de los datos, su geolocalización, la persistencia de los datos, su mezcla con otros clientes de la nube, los planes de recuperación de datos, el descubrimiento de datos y la agregación de los datos[446]. En definitiva como dice la ENISA muy gráficamente "la economía de escala y la flexibilidad del *cloud* son ambos un amigo y un enemigo desde el punto de vista de la seguridad"[447]. Los datos de Eurostat que hemos recogido anteriormente son un buen botón de muestra.

En la misma línea, pero de manera más desarrollada, un importante estudio de la consultora KPMG, señala que a la vez que existen importantes incentivos económicos –antes detallados- para la adopción del *cloud*, hay efectivamente algunas restricciones o riesgos que resumen en los siguientes puntos[448]: la velocidad y fiabilidad de los proveedores de servicios de telecomunicaciones; la compatibilidad de los procesos internos de la organización con las ofertas de la nube; la ubicación de los datos y las cuestiones concernientes a la seguridad y a la soberanía; la recuperación de los datos en caso de desastre; o el conocimiento limitado de las ofertas de productos y la falta de familiaridad de los negocios con las oportunidades[449], aspecto este último en el que resultan de nuevo útiles los datos de Eurostat antes mencionados.

---

explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises#Use_of_cloud_computing:_highlights

[444] Cabría un análisis SWOT (*Strengths, Weaknesses, Opportunities, Threats*) pero se ha preferido plantear los retos adoptando un lenguaje positive en pro de esta modalidad de computación.

[445] JANSEN, W. y GRANCE, T., Guidelines on Security and Privacy in Public Cloud computing. Ob. Cit.

[446] CLOUD SECURITY ALLIANCE. ob. cit. p. 21 y 22.

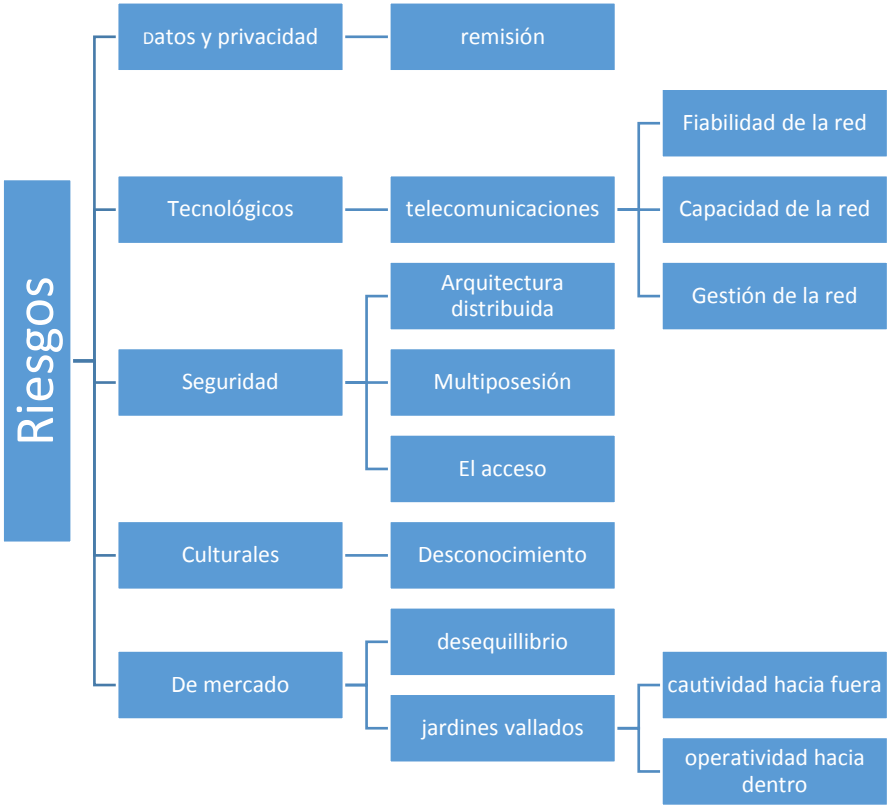
[447] ENISA. Cloud computing: Benefits, risks and recommendations for information security. Ob. Cit. p. 4.

[448] KPMG. ob. cit., p. 11.

[449] Debido a las características del estudio, enfocado al concreto caso de Australia, se afirma que esto último es predicable respecto de los negocios en este país. No obstante, se ha considerado fundamentado extender esta opinión de manera generalizada en la presente tesis.

Además de estos puntos señalados cabría añadir otros como los derivados del carácter multi-posesión o multi-arrendatario propio de la tecnología de la nube y, fundamentalmente de la interoperabilidad y la necesidad o no de estandarización en el desarrollo de esta nueva tecnología.

Al mundo específico de los datos dedicaremos el capítulo central de esta obra, por lo que aquí solamente quedarán apuntados, y a él nos remitimos. Sin embargo hay otros muchos aspectos que se encuentran alrededor de la computación en nube y en los que se enmarcan algunos de estos riesgos.



Fuente: elaboración propia

Hemos destacado más arriba que la tecnología del *cloud* es consecuencia del desarrollo de tecnologías propias, sin perjuicio, insistimos, de su sustantividad, y es por ello que el primero de los factores de riesgo es la necesidad de que exista un soporte en el plano de las telecomunicaciones para hacer frente a las exigencias de esta tecnología. El *cloud* en sí

mismo es la red. Sin esta no es posible aquella, sea Internet u otra. Este riesgo es además consustancial a cualquier modalidad de servicio y a cualquier modelo de implantación. Al ser un requisito en sí mismo de funcionamiento de cualquiera de ellos. Un fallo en la red impide el acceso a la información almacenada, una limitación en la capacidad de procesamiento, a la ejecución de programas…etc. Es una suerte de presupuesto ontológico. Sin red no hay nube. Muere la ubicuidad a la que hemos hecho mención anteriormente. Como dice David Cheriton, de la Universidad de Stanford "Creemos que Internet está siempre allí. Solamente por el hecho de que dependemos de Internet, no significa que eso es verdad"[450]. De hecho, la nube es la red en sí misma. Cualquier elemento de debilidad en la red, sea en términos de seguridad o en términos de capacidad, implica un riesgo en el primero de los casos y una debilidad en el servicio prestado en el segundo.

Organismos oficiales, doctrina y los propios proveedores de servicios en nube corroboran lo dicho. Así, el ONTSI ha señalado que un requisito para el funcionamiento del *cloud* es la universalización de la banda ancha, en la que juegan un papel clave las operadoras de telecomunicaciones[451]. Desde el punto de vista doctrinal, los profesores Geambasu, Gribble y Levy de la Universidad de Washington subrayan que la primera característica tecnológica clave para diferenciar el mundo de la nube del actual entorno de computación, junto con el sistema de almacenamiento compartido y los servicios de utilidades de cómputo remotos o servicios Web (*utility Web Services*), es precisamente una libre, eficiente y plena red de ancho de banda que soporte una integración de servicios de computación remotos más estrecha y a mayor escala que la que es posible a través de las Redes de Área Amplia (WAN en su acrónimo inglés)[452] que es una red que une dos o más redes de área local (LAN) con independencia de su ubicación física, elemento este que es consustancial a la nube. En cuanto a los proveedores, la empresa Microsoft por ejemplo ha hecho hincapié en la necesidad de que Europa tenga una infraestructura de comunicaciones adecuada para hacer frente a la tecnología *cloud* que incluiría una presencia más cercana de la fibra óptica a los domicilios de los consumidores pero también las tecnologías wireless van a jugar un papel

[450] CHERITON, D. Internet Arquitects Warn of Risks in Ultrafast Networks. *The New York Times*. 13 de noviembre de 2011.
[451] ONTSI. ob. cit. p. 54.
[452] GEAMBASU. R, GRIBBLE, S.D. y LEVY, H.M., CloudViews: Communal Data Sharing in Public Clouds. *Proc. Workshop Hot Topics in Cloud Computing (HotCloud).* 2009, article 14. Disponible en web: http://static.usenix.org/event/hot*cloud*09/tech/full_papers/geambasu.pdf

fundamental para conseguir que los beneficios del *cloud* sean genéricamente aprovechables[453].

En determinadas ocasiones los problemas pueden derivar del propio cálculo del proveedor de servicios en nube. En el caso de que se haya hecho una mala proyección de negocio y teniendo en cuenta las características bajo demanda del negocio del *cloud computing*, la situación puede llevar a la falta de disponibilidad del servicio, a que la confidencialidad esté comprometida e incluso los efectos que pudieran darse desde el punto de vista económico para la reputación del negocio. Pensemos por ejemplo en la Nochebuena de 2012 cuando los usuarios de Netflix no pudieron disfrutar de la programación debido a que hubo una sobrecarga en el sistema de Amazon, que prestaba el soporte y que se vio superado a su vez por un problema en una parte de su servicio (*Elastic Load Balancing*) que ayuda a diseminar el tráfico pesado entre sus múltiples servidores para prevenir la sobrecarga.

En conexión con esta fiabilidad y capacidad de la red está no solamente la capacidad de soportar las comunicaciones o el flujo de datos, para lo cual juega un papel fundamental el citado ancho de banda, sino también cómo se gestiona esa infraestructura de red. La gestión y la capacidad de gestión son algunos de los retos técnicos que afrontan los proveedores puesto que juegan un papel fundamental en algunas de las características esenciales del *cloud* (la elasticidad, la calidad del servicio, la adaptabilidad, la reducción de costes e incluso el factor "verde"). A título de ejemplo, se está comprobando que la gestión en los casos de una escalabilidad hacia arriba (*scale up*) es mejor que cuando son hacia abajo (*scale down*) puesto que en este último supuesto la duración de la inactividad es impredecible[454]. La escalabilidad hacia arriba supone coger lo que se tiene y sustituirlo por algo con mayor poder o capacidad. Desde el punto de vista de la Red, sería por ejemplo coger un computador de red de 1GbE y sustituirlo por uno de 10 GbE. El mismo número de puertos de conmutador, pero el ancho de banda ha sido escalado a través de mayores conductos. El cuello de botella de 1GbE ha sido aliviado por sus sustitución por uno de 10 GbE. La gestión en la red se convierte en un elemento esencial. Pensemos al respecto cómo en marzo de 2013, debido a un problema en los enrutadores periféricos de CloudFlare, cuyo servicio consistía en añadir

[453] SMITH. B, Building Confidence in the Cloud: A Proposal for Industry and Government Action for Europe to Reap the Benefits of Cloud computing. *European Commission. Contribution by Microsoft.* Bruselas, enero de 2010. Disponible en web: http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations/microsoft_corporation_2nd_document_en.pdf

[454] EUROPEAN COMMISSION. Expert Group Report*, The Future of Cloud computing. Opportunities for European Cloud computing Beyond.* ob. cit., p. 29.

una capa entre las casi 800.000 páginas web que gestionaban y sus usuarios de cara a acelerar el tráfico y prevenir ataque de denegación de servicios y otros aspectos de seguridad, se vieron afectados la totalidad de sus clientes.

En lo que concierne a los riesgos derivados de la seguridad, se debe señalar que la propia característica de una arquitectura distribuida conlleva mayor número de datos en circulación lo que hace que conductas como las del *sniffing* (se trata de una técnica por la cual se puede "escuchar" todo lo que circula por una red)*, spoofing* (se trata de una técnica por la que un atacante se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación para para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza con el suplantado)*,* un ataque *man-in-the-middle* o ataque de intermediario (se trata de una técnica en la que el atacante tiene la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas sea consciente), o un ataque de *replay* (técnica de ataque muy similar a la anterior) sean serias amenazas[455]. Hay que tener en cuenta que todas estas amenazas y muchas otras se dan tanto cuando los datos circulan en el entorno de la nube, algo necesario por su propia naturaleza y también por exigencias de calidad en el servicio, por ejemplo con la copias de respaldo; como cuando circulan entre el proveedor y el usuario o consumidor, perspectiva esta última que por cierto se olvida en muchas ocasiones y que puede ser uno de los elementos críticos de seguridad. De ahí la relevancia que adquieren los protocolos de acceso o las técnicas de cifrado a las que inmediatamente nos referiremos.

En el campo de los riesgos también se debe atender a los derivados de una de las principales notas del *cloud computing* cual es la del carácter multi-arrendatario y la compartición de recursos. La posibilidad de compartir recursos constituye una de las notas por excelencia de la arquitectura *cloud*. Permite la flexibilidad a la que nos referíamos. Sin embargo, dicha característica también comporta riesgos en caso de fallos en los mecanismos de separación del almacenamiento, la memoria, el enrutamiento e incluso la reputación entre los diferentes arrendatarios, por ejemplo a través de lo que se conoce como *guest-hopping atacks*, (se trata de una técnica mediante la cual un intruso ,interesado en los datos alojados en la máquina virtual A, pero que es incapaz de penetrar en ella de manera directa, intentará penetrar en la máquina virtual B, que se encuentre alojada en el mismo hardware, y a través de ella intentar acceder a la otra.). El riesgo viene dado por el propio atractivo que genera la posibilidad de

[455] *Idem,* ob. cit., p. 37

acceder a un mayor volumen de información en el marco de un mismo ataque. Parafraseando a Willie Sutton, ¿Por qué atacar los centros de datos? Porque es allí donde están los datos. Además los problemas de esa naturaleza compartida se pueden dar también incluso cuando la intervención venga amparada por actuaciones legales. Pensemos por ejemplo en el cierre de la conocida página de intercambio de archivos Megaupload a principios de 2012 que, si bien resultaba necesaria en cuanto a la masiva vulneración de derechos de propiedad intelectual que en ella se ejecutaban, sin embargo tuvo el efecto negativo de que la orden de cierre dejó a muchos usuarios sin la posibilidad de acceder a archivos totalmente legítimos que tenían en ella almacenados. O de similar modo cuando el 21 de junio de 2011 el FBI embargó el hardware en un centro de datos en Reston que afectó no solamente a los tres servidores afectados por la redada sino a otros 59 más, lo que inutilizó 160 páginas web que no tenían nada que ver con el caso[456].

En todo caso la ENISA señala que los ataques a mecanismos de aislamiento de recursos (por ejemplo contra los hipervisores[457]) son mucho más difíciles comparados con los ataques a los sistemas operativos tradicionales[458]. Esa misma arquitectura es la que puede dar lugar a problemas en cuanto al borrado de los datos puesto que es posible que no se pueda hacer debido a que el disco que los aloja contenga también datos de otros clientes[459].

A los riesgos señalados se añaden los que nosotros denominados problemas de naturaleza cultural. Ya hemos apuntado que las PYMES son sin duda uno de los principales potenciales beneficiarios del uso de este tipo de tecnología. También al analizar las ventajas de uno y otro modelo de implantación, por la diferencia que existe respecto al coste de entrada, hemos visto que la tendencia será hacia el uso de la nube pública frente a la privada. Sin embargo, en cuanto que cliente no experto, en numerosas ocasiones existirá un desconocimiento

---

[456] SWARTZ, M.J. *Are* You Ready For An FBI Server Takedown? *Network Computing*. 7 de enero de 2011. Disponible en web: http://www.networkcomputing.com/government/are-you-ready-fbi-server-takedown/1418400854

[457] Siguiendo a Tim Jones, podemos definir los hipervisores "Los hipervisores son a los sistemas operativos lo que los sistemas operativos, en cierta medida, son a los procesos, es decir, proveen plataformas de hardware virtual aisladas para ejecución, que, a su vez, dan la ilusión de tener acceso total a la máquina subyacente. Se oculta el hardware físico subyacente de manera tal que pueda ser usado y compartido entre múltiples sistemas operativos de manera transparente", en JONES, T. La anatomía de un hipervisor Linux [en línea]. *IBM Developer Works.* 31 de mayo de 2009. Es cierto que cabría la posibilidad de que la separación o "frontera de seguridad" fuera física (es decir que estuvieran los datos de los clientes del proveedor almacenados en hardware diferente), pero lo habitual es que lo estén a través de fronteras virtuales mediante el uso de compartimentos virtuales. MICROSOFT. A guide to Data Governance for Privacy, Confidentiality, and Regulatory Compliance. Part 5: Moving to cloud computing. agosto de 2010, Disponible en web: http://www.microsoft.com/privacy/datagovernance.aspx

[458] ENISA, ob. cit., p. 10.

[459] *Idem*, p. 10.

respecto a las ventajas que puede aportarle un sistema de este tipo y, lo que es más relevante, respecto al modo en que funciona. Ya hemos apuntado que la nube resulta oscura para el cliente que no conoce cómo funciona desde el punto de vista tecnológico y en muchas ocasiones bajo qué paraguas normativo lo hace. Eso puede dar lugar por ejemplo a que se esté consintiendo el uso de la información almacenada para una finalidad diferente al propio proveedor bajo esa apariencia de gratuidad a la que hemos hecho mención. O que se desconozca por ejemplo la ubicación de los datos, o el número de personas que van a poder acceder a la información, o la localización geográfica de la misma. Bajo esa apariencia que consigue la nube, bajo esa sensación de cercanía al cliente que conlleva la ubicuidad, se pueden estar produciendo problemas de gran calado referidos a la propiedad de la información, a la normativa que resultará aplicable, a accesos no sospechados por parte del cliente…etc. Es una suerte de efecto anestesia que el cliente tiene. Una de las grandes ventajas del cliente, el acceso sin necesidad de conocimientos técnicos a alta tecnología y también a importantes mecanismos de seguridad, sin embargo tiene como contrapartida un sometimiento a un tercero que en determinadas ocasiones puede afectar a elementos críticos.

En línea con este sometimiento que mencionamos, se ubicaría otro de los problemas cual es del denominado cliente cautivo. Si bien algo hemos apuntado en el capítulo anterior y aunque lo desarrollaremos de una manera detallada al tratar del derecho a la portabilidad de los datos en la nube en el próximo capítulo, no podemos dejar de hacer una sucinta mención porque constituye, a medio y largo plazo, uno de los grandes riesgos que asume el cliente que se "sube" a la nube. El problema viene dado por el carácter cerrado de las nubes que existen y se están construyendo. Al igual que en otras tecnologías, podemos estar ante una nueva forma de "*lock-in*" (la denominada encerrona tecnológica). Esta misma línea la sostiene Zittrain al afirmar que cuando conferimos nuestras actividades e identidades en un lugar en la nube, conlleva mucha insatisfacción luego movernos[460]. Se trata de la conocida doctrina de los "jardines vallados" que plantean los retos de la estandarización, la migración y en definitiva la interoperabilidad necesaria para el desarrollo de Internet en general y del *cloud* en particular, guardando, eso sí, el lógico equilibrio con la innovación. La estandarización, la interoperabilidad, la ausencia de neutralidad, la posibilidad de ejecución de aplicaciones en entornos operativos de otro proveedor, la posibilidad de mover nuestros archivos con libertad…son problemas que siempre han estado ahí, en el núcleo mismo de la

[460] ZITTRAIN, J. Lost in the Cloud*. New York Times.* July 20th, 2009*.*

red, pero que en el ámbito del cloud, donde se pone en manos de terceros no solo el flujo sino la información en sí misma, puede tener graves consecuencias. Pensemos que esa voluntad de cambio en el servicio no puede venir dada únicamente por razones de mercado (mejor precio, mayor personalización del servicio…) sino que puede venir dada por razones críticas (quiebra del proveedor, fallos en la seguridad, centros de datos en zonas de conflicto…etc.).

Además, la falta de estandarización puede provocar también problemas para la integración con otros subsistemas de negocio que se requieran mantener en modo tradicional en una compañía[461] y con los procesos internos a los que antes hemos hecho mención. No podemos olvidar que el salto a la nube puede ser total o solamente parcial. En determinadas ocasiones se puede querer, e incluso es conveniente, conservar determinados ámbitos *in house*. Como toda prestación de servicios, no es infrecuente que la parte más nuclear de un determinado negocio se mantenga dentro de la estructura interna de la compañía. Cabe la posibilidad de que los datos de una misma empresa en función de su nivel de criticidad puedan radicar en una nube pública, otros en una nube privada y los datos más críticos se mantengan sin embargo en un almacenamiento interno en los propios servidores de la empresa. Es por ello que se hace necesario verificar que el coste de adaptabilidad, de interoperabilidad entre el servicio provisto por la nube y la estructura interna de la organización, no sea superior al ahorro de costes derivado del salto a la nube. La nube como panacea puede derivar en un quebradero de cabeza interno si la falta de interoperabilidad afecta a los procesos de negocio.

La falta de compatibilidad o interoperabilidad trae causa también de otro de los problemas existentes en el mercado y es el de la falta de equilibrio generalizada entre proveedores y clientes; debida a la propia naturaleza de los proveedores, que exigen en muchas ocasiones de una estructura al alcance de pocas empresas tecnológicas (de ahí que sea tan frecuente el fenómeno de la subcontratación); como de la naturaleza del negocio en sí mismo, que incrementa beneficios mediante las soluciones estandarizadas. Este desequilibrio conlleva que la personalización de las soluciones tecnológicas a cada cliente tenga un alcance limitado, incluso en el seno de las nubes privadas, aunque en estas lógicamente sea mayor. Más allá de las implicaciones jurídicas que esta vertiente tiene, y que se tratarán en el próximo capítulo, esta situación conlleva en muchas ocasiones que quien contrata los

[461] ONTSI, ob. cit., p. 55.

servicios lo tenga que hacer en su totalidad, por la potencial falta de compatibilidad con su operativa interna, lo que puede incluso acabar derivando en modificaciones de sus procesos de negocio. En definitiva se puede pasar de verse favorecido por un determinado servicio, a adaptar el negocio a las características del servicio ofrecido. *Take it or leave it* resumiría muy bien la situación. Es decir, en el cloud se paga por lo que se necesita, pero lo que se necesita viene determinado en muchas ocasiones por el propio proveedor y no por el cliente.

Algunas de las notas características que hemos señalado, como la arquitectura distribuida o la ubicuidad, son las que hacen que se pueda acceder a la nube y a lo que ella contiene desde infinitos puntos de acceso, por lo que los protocolos que determinan cómo acceder y quién puede acceder, son determinantes. Si a ello se añade la cadena de subcontrataciones que puede necesitar un servicio en nube, aumenta este riesgo exponencialmente. Por ejemplo, el profesor Areitio, de la Universidad de Deusto señala como uno de los principales retos en seguridad del *cloud computing* las necesidades de cifrado: cifrado para el acceso a la interfaz de control de recursos de la red, cifrado administrativo de acceso a las instancias de sistemas operativos, cifrado de acceso a las aplicaciones y el cifrado de los datos de las aplicaciones en reposo, almacenamiento y tránsito[462]. En este punto hay que destacar que a juicio de reconocidas autoridades como la Dra. Cavoukian, sin una mejor gestión de la identidad digital no estaremos en disposición de asegurar a los usuarios individuales que pueden migrar con seguridad sus datos críticos y sus aplicaciones de sus ordenadores a la Web[463]. Empresas del sector como Microsoft afirman igualmente que el control de acceso y la identidad están entre las tareas tecnológicas más complejas, a la par que tiene enormes consecuencias directas en la protección de la información. A lo que se añaden además otras cuestiones vinculadas como el hecho de que el entorno de identidad debe ser interoperable entre las aplicaciones que exigen de esa identidad y debe ser gestionable por la organización que está pagando el servicio[464]. Se trata de determinar quién de los subcontratados va a poder acceder a la información, qué papel le corresponde a potenciales colaboradores externos del proveedor, a las personas encargadas del mantenimiento, de cómo las normas laborales han de profundizar en la elaboración de códigos de conducta que fijen claramente las normas de acceso, tanto respecto a los dispositivos y redes a través de los cuales se puede realizar, como respecto a la gestión de las contraseñas o mecanismos de identificación y autenticación. Se trata en definitiva de que todos los eslabones de la cadena

[462] AREITIO, J. ob. cit., p. 47.
[463] CAVOUKIAN, A. ob. cit., p. 6.
[464] MICROSOFT. ob. cit., p. 9.

que se conforma alrededor de una organización que migra su información a la nube, sean lo más robustos posibles. Al igual que señalábamos anteriormente la importancia de la relación entre el cliente y el proveedor es olvidada en numerosas ocasiones, dedicándose los análisis al estudio de la nube propiamente dicha y de su entorno. Muchas veces se pierde la perspectiva de que con independencia de que el almacenamiento, el procesamiento o el desarrollo se estén llevando a cabo en la nube, el acceso a la misma se está realizando a través de muy diversos dispositivos. La nube se caracteriza por un camino de ida y vuelta o, si se prefiere, por un camino circular que comienza en un determinado dispositivo, pasa por la nube y vuelve a ese mismo o a otro dispositivo distinto. Por todo ello es fundamental evaluar toda la cadena de servicio evitar defectos en el diseño y en la propia prestación del servicio[465]. En particular por ejemplo el aprovisionamiento de identidad donde se hace absolutamente necesario que el proveedor de servicios en nube integre sus prácticas tecnológicas con las de la empresa o el cliente de modo que no existan lagunas de seguridad[466]. Pensemos por ejemplo en el caso de Dropbox en 2011 cuando se pudo, durante cuatro horas, acceder a su contenido mediante la introducción simplemente de la dirección de correo electrónico y sin necesidad de introducir ningún tipo de contraseña, que era meramente opcional. O también, en el caso por ejemplo de Joyent en mayo de 2014 cuando uno de los responsables de mantenimiento que iba a llevar a cabo una actualización de algunos de los servidores de un centro de datos en el este de Estados Unidos, debido a un error, introdujo un código que conllevó que se actualizarán y reiniciaran todos los servidores del centro de datos a la vez, por lo que el centro de datos dejó de prestar servicios a todos sus clientes entre 20 minutos y dos horas y media…Un solo administrador pudo echar abajo todo el servicio.

Para culminar nos encontraríamos con los riesgos concernientes a la privacidad y que van a constituir, como ya se ha adelantado el núcleo de este trabajo. Estamos hablando de aspectos como la responsabilidad que asume cada uno de los sujetos que participa del contrato; de cómo la determinación de la normativa aplicable y la jurisdicción competente vendrán determinados en parte por la ubicación geográfica de dichos datos; de cómo el carácter transnacional de la nube, que es nota característica en muchas ocasiones, hace determinante el régimen de las transferencias internacionales de datos; de cómo las cadenas de subcontrataciones, como se ha apuntado, no debiliten la necesaria robustez de la

[465] *Idem* ob. cit., p. 10.
[466] *Ibidem.* ob. cit., p. 16.

seguridad; de cómo las medidas de seguridad aplicables se correspondan con la criticidad de la información; de que se apliquen unos criterios de transparencia que expongan claramente las posibilidades de acceso a la información por parte de las autoridades púbicas. En definitiva, se trata de que la totalidad del ciclo de los datos que son tratados en la nube, esté protegido, para que los beneficios que hemos visto puede potencialmente tener esta tecnología no se vean mermados porque uno de los retos derive en riesgo por superar determinados umbrales, y consiguientemente puedan concluir en una conculcación de la privacidad del cliente del proveedor o de los clientes de aquel. En el resto de la obra nos vamos a dedicar a analizar los aspectos del ciclo de vida de la protección de datos que se ven más tensionados en el entorno de la computación en nube. Y sobre todo, se va a dar respuesta en cada uno de ellos a si los instrumentos de que nos dota el actual régimen jurídico resultan válidos o no para hacer frente a los retos planteados. En caso de que resulten válidos, se verá si lo resultan en sus propios términos o es necesaria una cierta flexibilidad. En caso de que no resulten válidos, se indicará cuál podría ser el tratamiento normativo más adecuado.

"Do not be confused. Clouds are not a data protection free zone"
Stewart Dresner, Chief Executive, Privacy Laws & Business

"Cloud Computing es una trampa destinada a obligar a la gente a adquirir sistemas propietarios, bloqueados, que costarán más conforme pase el tiempo"
Richard Stallman, EFF

CAPÍTULO III: LOS ELEMENTOS SUBJETIVOS DE LA PRIVACIDAD EN LA NUBE

1 Normativa aplicable a la computación en nube

Paso previo al análisis del régimen jurídico de la protección de datos en la nube, procede abordar una de las grandes dificultades en Internet que es saber qué legislación resultará aplicable en cada caso concreto. Cuando los datos se encuentran almacenados en el PC de la empresa o del usuario correspondiente, está claro que la legislación aplicable es la del lugar donde se encuentra radicado dicho hardware. Sin embargo, en la nube, los elementos definidores de la Teoría Clásica del Estado –territorio, población y poder[467]– se ven claramente desbordados y desnaturalizados. Como señalan los profesores Newman y Andrews, la concepción de los Estados nación basada en el territorio puede devenir rápidamente arcaica en un mundo crecientemente conectado[468]. En la nube nos podemos encontrar con que la información puede haber sido creada en Francia, utilizando software almacenado en Polonia, procesada en el Reino Unido, almacenada en Irlanda y accesible en Letonia por ciudadanos italianos[469]. La cuestión más importante es que el cliente sepa dónde están almacenados y dónde son procesados sus datos[470] o, estrechando el círculo,

[467] Cualquiera de los autores clásicos como Jellinek, Heller, Hauriou, Diguit o Carré de Malberg recogen, con diferentes matices, estos elementos.
[468] ANDREWS, D.C. y NEWMAN, J.M. Personal Jurisdiction and Choice of Law in the Cloud. *Maryland Law Review.* 2013, vol. 73, Issue 1, p. 313-384. Disponible en web: http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3605&context=mlr
[469] SMITH, B. ob. Cit.
Por su extensión, no recogemos el ejemplo que viene en el siguiente artículo pero que para quienes estén interesados, refleja muy bien la complejidad de lo que estamos hablando. REINGOLD, B., MRAZIK R. y D'JAEN, M. Cloud Computing: Whose Law Governs the Cloud? (Part III). Cyberspace Lawyer. January-February 2010, p. 1-6. Disponible en web: https://www.perkinscoie.com/images/content/2/1/v2/21576/sea-10-03-westlaw-document-09-48-34.pdf
[470] EUROPEAN DATA PROTECTION SUPERVISOR. Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe. 2012. p. 4. Disponible en web:

en el marco de qué actividades se están tratando. Entre otros motivos, es muy importante porque eso será determinante de qué norma se aplica. Lo más relevante es cuando la normativa que se aplica es la de la Unión Europea ¿Por qué? Porque la legislación europea es la más exigente en materia de protección de datos[471].

El siguiente cuadro comparativo, enfocado al mundo asiático, pero incluyendo datos de la Unión Europea y de Estados Unidos, pone de manifiesto esta realidad de Europa como el ámbito geográfico más desarrollado en materia de protección de datos, algo que en gran medida responde al enfoque con que se afronta su regulación en cada caso[472].

https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf

[471] A título de ejemplo y desde el bufete australiano *Truman Hoyle* se ponen numerosos ejemplos de problemas derivados de diferentes niveles de exigencia en materia de protección de datos. Así señalan, entre otras, cómo en el caso del Reino Unido cuando HSBC fue sancionada con una multa de tres millones de libras esterlinas por un fallo de seguridad en los datos confidenciales de sus clientes. Tomado de VINCENT, M. y HART, N. Cloud Computing-Legal Issues in the Cloud. Truman Hoyle Lawyers. *Mondaq*. 26 de octubre de 2010. Disponible en web: *http://www.mondaq.com/australia/x/113912/Cloud+computing+legal+issues+in+the+cloud,*

[472] Un buen resumen de esa comparativa entre diferentes regiones en las primeras páginas de TIKK-RINGAS, E., SPIRITO, C., HUSAIN, A. y AL-TAYEB, I. Considerations for regulatory and policy approaches to Cloud Computing in the GCC. *IISS White Paper.* 2013. Disponible en web: https://www.iiss.org/en/events/events/archive/2013-5126/may-6ac8/cloud-is-no-limit-data-security-solutions-in-the-uae-ab22/white-paper-b137

Country	General law on personal data privacy protection	Separate regulator	Register of data controller	Sector-specific regulation	"White list" countries or requirement on data controllers to ensure protection on data transfers	Individual consent required for data transfers	Contract obligations accepted as reason for data transfers	Companies required to appoint 'Data Protection Officer'
Australia	Y	Y	Y	Y	Y	Y	Y	N
New Zealand	Y	Y	N	Y	Y	Y	Y	Y
India	N	N	N	Y	Y	Y	Y	Y
Indonesia	Proposed	N	N	Y	N	Proposed	N	N
Hong Kong	Y	Y	Y/N	Y	Y/N	Y	Y	N
Japan	Y	N	N	Y	Y	Y	Y	N
Malaysia	Y	Y	Y	Y	Y	Y	Y	N
Philippines	Y/N	Y/N	N	Y	Y	Y	Y	Y
Singapore	Y	Y	N	Y	Y	Y	Y	Y
South Korea	Y	N	N	Y	Y	Y	Y	Y
Taiwan	Y	N	N	Y	Y	Y	Y	N
Thailand	Y	N	N	Y	Y	Y	Y	N
EU	Y	Y	Y	Y	Y	Y	Y	Proposed
UK	Y	Y	Y	Y	Y	Y	Y	Y
USA	N	FTC	N	Y	N	By sector	Y	Varies

Note: (i) Y/N means it is on the stature book but not yet implemented.

Fuente: *Asia Pacific Carriers' Coalition (APCC) and The Asia Cloud Computing Association (ACCA), 2014*[473]

Precisamente esta circunstancia ha conllevado que con la finalidad de evitar estar sometida a diferentes niveles de protección y a un entramado laberíntico de normas y jurisdicciones, muchas compañías proveedoras de servicios *cloud* hayan introducido una suerte de "cláusula europea" u opción de "restricción territorial"[474], en virtud de la cual existe un compromiso de que los datos no serán procesados ni almacenados fuera de territorio de

[473] ASIA CLOUD COMPUTING ASSOCIATION y ASIA PACIFIC CARRIERS COALITION. Report on Cloud Data Regulations. A contribution on how to reduce the compliancy costs of Cross-Border Data Transfers. 2014. Disponible en web: http://trpc.biz/wp-content/uploads/APCC-ACCA_WhitePaper_CloudRegulations_2014_FullPaper.pdf

[474] MAYER BROWN. Cloud Computing May Violate German Data Privacy Laws. 20 de julio de 2010. Disponible en web: http://www.mayerbrown.com/files/Publication/aef6b505-6895-43b2-9bf8-6d1423e5a61d/Presentation/PublicationAttachment/b31735d9-fc20-4e67-a5db-79d6cd77f659/WORD_Cloud-Computing_0710_V1.pdf,
Ver también VINCENT, M. y HART, N. Cloud Computing-Legal Issues in the Cloud. *Journal for the Australian and New Zealand Societies for Computers and the Law.* January 2011, nº 79, p. 1-6. Disponible en web: http://www.austlii.edu.au/au/journals/ANZCompuLawJl/2011/1.pdf

aplicación de la norma comunitaria. A título de ejemplo Google o Amazon, por señalar dos de los más importantes proveedores a nivel mundial, lo ofrecen[475].

¿Y cuándo se aplica la normativa europea?[476] La Directiva 95/46 recogía el ámbito de aplicación en su art. 3, pero referido exclusivamente al ámbito "material" de aplicación. Es el art. 4 por su parte el que puede resultar de utilidad en el sentido de que fija los criterios físicos o espaciales sobre los cuales se delimitaba la normativa aplicable. En concreto establece que los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:

a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro;
b) el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público;
c) 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.

En definitiva parecen claros los dos criterios aplicables: o bien el responsable está radicado en un Estado miembro, o bien sin estarlo utiliza para el tratamiento medios radicados en un

[475] Respecto del primero se informa en el siguiente documento: PINSENT MASONS. Google's cloud database management service offers EU-only data storage and processing. Disponible en web:, http://www.out-law.com/en/articles/2012/november/googles-cloud-database-management-service-offers-eu-only-data-storage-and-processing/, mientras que del segundo lo hace el documento mencionado en la nota anterior, p.2.

[476] Hay quienes sostienen, caso de los citados profesores Andrews y Newman, que "simplemente preguntarse si resulta o no aplicable la normativa local no es suficiente, particularmente dada la creciente naturaleza nacional e internacional del *cloud computing.* ANDREWS, D.C. y NEWMAN, J.M. ob. cit, p. 379. En la medida en que el tratamiento en un entorno cloud conlleva el tratamiento de datos personales en conexión con la provisión de servicios de comunicación electrónica accesibles al público en redes de comunicación públicas (operadores de telecomunicaciones), el tratamiento deberá también cumplir con 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). Para ver un detallado estudio de esta cuestión, la tesis doctoral de Malentina Pavel Burloiu en la Universidad de Tilburg, PAVEL BURLOJU, M. *Cloud computing and the regulatory framework for telecommunications and information society services*. Tilburg University. febrero de 2012. En particular páginas 47 y siguientes. Disponible en web: http://arno.uvt.nl/show.cgi?fid=121935

Estado miembro. Así parece también afirmarlo el Supervisor Europeo de Protección de Datos (en adelante SEPD)[477].

No estaba previsto expresamente, por obvias razones del devenir tecnológico y de la cronología normativa, qué criterio se había de utilizar para la determinación de la normativa aplicable en los supuestos en que un cliente contrata a un prestador de servicios en nube. Sin embargo, siguiendo por analogía dichos criterios, de manera inicial cabría resaltar que se da en dos supuestos concretos: cuando el prestador de servicios en nube actuando como responsable está establecido en la Unión Europea o actúa para un responsable de los datos establecido en territorio de la Unión Europea (derivado del art. 4.1 a) de la Directiva); o bien cuando igualmente como responsable utilice unos medios establecidos en un Estado miembro o actúe como encargado del tratamiento de los datos de un responsable utilizando ese equipamiento (derivado del art. 4.1 c) de la Directiva)[478]. En el resto de los casos no está obligado por la normativa comunitaria[479].

En línea con lo fijado, lógicamente, por la normativa comunitaria, y de conformidad con lo establecido por el art. 2.1 de la LOPD, se aplicará la LOPD a los servicios prestados en nube cuando se dé cualquiera de estas dos circunstancias[480]: cuando el prestador de servicios en nube esté establecido en España o actúe como encargado del tratamiento para un responsable del tratamiento establecido en territorio español; o cuando el prestador de servicios en nube utilice medios establecidos en España o actúe como encargado del tratamiento de los datos de un responsable que utilice ese equipamiento. Hay que introducir alguna regla añadida que contempla el ROPD como lo previsto en el párrafo segundo del artículo 3.a) respecto a que cuando exista un encargado del tratamiento ubicado en España, serán de aplicación al mismo las normas concernientes a las medidas de seguridad; o lo

[477] EUROPEAN DATA PROTECTION SUPERVISOR. Opinion on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe. Ob. Cit. p. 7.

[478] Ver a este respecto el documento del ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 8/2010 on applicable law. diciembre de 2010. Disponible en web: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf

[479] No faltan voces autorizadas como las de Peter Hustinx, quien fuera Supervisor Europeo de Protección de Datos, que señalan la necesidad de incorporar nuevos criterios como en aquellos casos en los que el principal campo de negocio esté en Europa. Como luego veremos, la redacción del RGPD ha incorporado en gran medida este criterio. HUSTINX, P. Data protection and Cloud Computing under EU law. *Third European Cyber Security Awareness Day.* 13 April, 2010. Disponible en web: *http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-04-13_Speech_Cloud_Computing_EN.pdf*

[480] En su documento sobre "Cloud computing. Protección de datos personales", Ricard Martínez, Coordinador del Área de Estudios de la Agencia Española de Protección de Datos dice que "cuando un responsable de fichero o tratamiento en España contrata servicios de Cloud Computing aplicará los principios y obligaciones de la LOPD".

previsto en el artículo 3.c) del ROPD que contempla que cuando el responsable no esté radicado en territorio español pero use equipamiento para fines distintos de los de mero tránsito, deberá designar un representante.

Responsable radicado en territorio UE	**Prestador de servicios fuera de la UE**	**Aplicación normativa europea (art. 4.1.a)**	**El responsable exporta su legislación al encargado**
Responsable radicado fuera de territorio de la UE	Prestador de servicios en territorio UE	Aplicación normativa europea (art. 4.1.c)	El encargado exporta su legislación al responsable
Responsable radicado fuera de territorio UE	Prestador de servicios fuera de la UE	No aplicación de la normativa europea	

Fuente: elaboración propia[481]

En definitiva, la aplicabilidad extraterritorial de las normas que se deriva del referido cuadro se puede decir que es un elemento consustancial a la computación en nube. De hecho, como apunta Naranayan, existen diferentes principios competenciales del Derecho Internacional que pueden justificar una regulación efectiva del cloud computing: la competencia extraterritorial está permitida salvo que una norma internacional lo prohíba, la normativa de protección de datos pertenece más al Derecho Público que al Derecho Privado, y todo ello

[481] Ver al respecto el GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 5/2012 sobre la computación en nube. 2012. Disponible en web: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_es.pdf
En particular lo señalado en las páginas 8 y 9,

siempre que el ejercicio de la competencia sea "razonable"[482]. Si bien el mismo autor reconoce que la vía por excelencia es la de la cooperación internacional[483].

En este punto hay que considerar que la cuestión de la aplicabilidad de la normativa comunitaria puede ser todavía de mayor complejidad a la vista de algunos conceptos y la dificultad interpretativa a que han dado lugar algunos como "marco de actividades" , "establecimiento" o "medios", que son utilizados por el artículo 4 de la Directiva[484]. Analicemos cada uno de estos conceptos que pueden ser clave a la hora de determinar la normativa aplicable en el caso del *cloud computing*.

En referencia al concepto de establecimiento, el Grupo de Trabajo del artículo 29 en su Opinión 8/2010 y siguiendo la doctrina marcada por el Tribunal de Justicia[485], entre otros afirma que un servidor u ordenador no es probable que se califique como tal ya que se trata de una simple herramienta o instrumento técnico para el tratamiento de información; mientras que la oficina de una persona se calificaría en la medida en que haga algo más que simplemente representar a un responsable del tratamiento establecido en otro lugar y esté activamente implicada en las actividades en cuyo marco se efectúe el tratamiento de datos personales[486].

---

[482] NARAYANAN, V. Harnessing the Cloud: International Law. Implications of Cloud-Computing. *Chicago Journal of International Law*, 2012, vol. 12, nº 2, p. 783-809. Disponible en web: http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1629&context=cjil En este artículo el autor pone de manifiesto como muchos de los criterios que sienta el Derecho Internacional son de máxima utilidad a la hora de justificar tanto la aplicabilidad de normas como cuestiones de jurisdicción extraterritorial. Sin que sea de manera exhaustiva cita: el principio de territorialidad objetiva (que incluye la doctrina de los efectos, de particular importancia para Internet como pusieron de manifiesto los casos Yahoo o Toben; el principio de territorialidad subjetiva; el principio de nacionalidad, particularmente complejo en cuanto a la nacionalidad corporativa o empresarial; el principio de personalidad o nacionalidad pasiva, con particular incidencia en el ámbito penal; el principio protector;

[483] *Idem,* p. 801. Resulta interesante el análisis que el autor lleva a cabo y que estudia cuatro aspectos: las restricciones que determinados acuerdos internacionales pueden conllevar, modelos de armonización existentes como el de la propiedad intelectual; que hubiera una organización internacional única dedicada a la promulgación o examen de la regulación del cloud; o que los proveedores estuvieran sometidos a diferentes normas en diferentes partes del "espacio de la nube", recurriendo a la Convención sobre el Derecho del Mar como un instrumento de análisis de esta idea, págs. 802 y siguientes.

[484] Un muy interesante tratamiento de esta cuestión se observa en KUAN HON, W., HÖRNLE, J. y MILLARD, C. Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing. *International Review of Law, Computers & Technology*. 2012, vol. 26, Iss. 2-3, p. 129-164. Disponible en web: http://www.tandfonline.com/doi/full/10.1080/13600869.2012.698843?scroll=top&needAccess=true

[485] ARTICLE 29 DATA PROTECTION WORKING GROUP. Opinion 8/2010 on applicable law. Ob. cit. p.13 y 14.

[486] Resulta en este sentido particularmente llamativa la Sentencia que se dictó en Italia contra tres ejecutivos de Google a los que se condenó a seis meses de prisión por vulneración de la intimidad, considerándoles responsables tras haberse publicado en Google Video un clip de un conjunto de jóvenes maltratando a otro con síndrome de Down.

Recurriendo a la interpretación auténtica, únicamente contamos con el Considerando 19 en el que se dice que "el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable; que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante al respecto…". En el caso de la normativa española sí que contamos con dicha definición, por cuanto el artículo 3.2 ROPD dice: "A los efectos previstos en los apartados anteriores, se entenderá por establecimiento, con independencia de su forma jurídica, cualquier instalación estable que permita el ejercicio efectivo y real de una actividad". También, en el marco del ordenamiento español, resulta de utilidad el artículo 2.2 LSSI que señala que "resulta de aplicación la citada Ley cuando la sociedad, aunque no tenga su domicilio en España, opera mediante establecimiento permanente en España entendiendo que existe establecimiento permanente cuando disponga en España, de forma continuada o habitual, de instalaciones o lugares de trabajo, en los que realice toda o parte de su actividad". Por último, merece señalarse la Sentencia del TJUE de 1 de octubre de 2015[487], en el caso *Weltimmo s. r. o. vs. Nemzeti Adatvédelmi és Információszabadság Hatóság,* en la que se sostiene, en palabras de la propia Sentencia, "*una concepción flexible de la noción de establecimiento, que rechaza cualquier enfoque formalista*". Poco o nada nos aporta aquí el nuevo RGPD, ya que su artículo 4 que contiene las definiciones, solamente habla de la de establecimiento principal, más preocupado por la aplicación coherente y la jurisdicción de autoridades que por la aplicabilidad de la norma en sí misma.

A nuestro juicio incluso, se consideraría establecimiento cuando se dé la propiedad o exista una suerte de arrendamiento total, es decir, en aquel supuesto en el que las instalaciones pueden no ser propias pero los empleados encargados de su gestión y mantenimiento son del responsable del tratamiento y no de un tercero. En el caso de que confluyan estos

Italia. Tribunal ordinario de Milán (Sección 4ª de lo Penal). Sentencia de 24 de febrero de 2010. El acceso a la Sentencia del Tribunal Supremo en italiano en el siguiente enlace: http://www.giurcost.org/casi_scelti/Google.pdf
Finalmente el Tribunal Supremo italiano confirmó la revisión de la Sentencia del tribunal de apelación de Milán. Italia. Tribunal ordinario de Milán. Sentencia de 24 de febrero de 2010. El acceso a la Sentencia del Tribunal Supremo en italiano en el siguiente enlace: http://www.giurcost.org/casi_scelti/Google.pdf

[487] Unión Europea. Tribunal de Justicia de la Unión Europea. Caso Weltimmo s. r. o. vs. Nemzeti Adatvédelmi és Információszabadság Hatóság (C-230/14). Sentencia de 1 de octubre de 2015. Acceso al texto de la Sentencia en español en el siguiente enlace: http://curia.europa.eu/juris/document/document.jsf?text=&docid=168944&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=182564

supuestos cabría la consideración de establecimiento a efectos del artículo 4.1.a) de la Directiva y 2 de la normativa española.

En lo que en concreto nos ocupa sin embargo, hemos afirmado que el concepto de establecimiento no es aplicable a un servidor o a un ordenador. Sin embargo ¿resultaría aplicable a un centro de datos o a una granja de servidores en territorio UE de que dispusiera una empresa que no estuviera radicada a su vez en territorio comunitario pero que lo utilizara para servicios en nube? Hay que tener en cuenta que estos constituyen, desde el punto de vista físico, uno de los elementos centrales para una adecuada prestación de servicios en nube. Los centros de datos pueden ser hoy día granjas de servidores a una escala masiva

Fuente: elaboración propia con base en información suministrada por *Asian Cloud Computing Association*[488]

¿Constituye un centro de datos o una granja de servidores establecida en un Estado Miembro y utilizada para prestar el servicio un "establecimiento" en el sentido de la Directiva? ¿Estaríamos solamente ante elementos de naturaleza técnica y consiguientemente ante un "equipamiento" o unos "medios"? A nuestro juicio estamos ante equipamientos de naturaleza técnica[489]. El hecho de que en dicho centro de datos exista una labor de dirección, gestión o

[488] ASIA CLOUD COMPUTING ASSOCIATION y ASIA PACIFIC CARRIERS COALITION. Report on Cloud Data Regulations. A contribution on how to reduce the compliancy costs of Cross-Border Data Transfers. Ob. Cit. p. 8.

[489] Así parece también confirmarse en el ejemplo 5 que utiliza el GT del artículo 29 en su Dictamen 8/2010. Un proveedor de servicios de Internet (el responsable del tratamiento de datos) tiene su sede central fuera del territorio de la UE, por ejemplo en Japón. Tiene oficinas comerciales en la mayoría de los Estados miembros de la UE y una oficina en Irlanda que gestiona los temas relacionados con el tratamiento de los datos personales, entre los que figura, en particular, el apoyo informático. El responsable del tratamiento está desarrollando un centro de datos en Hungría, en el que los empleados y los servidores se dedican al tratamiento y almacenamiento de datos relativos a los usuarios de sus servicios. El responsable del tratamiento de Japón tiene asimismo otros establecimientos en varios Estados miembros de la UE con diferentes actividades. Al margen de otras consideraciones de relevancia, en lo que nos interesa, se

mantenimiento no implica que pierdan dicha virtualidad porque tienen precisamente ese enfoque técnico y no entran en la determinación de los fines y de los medios del tratamiento en el sentido que más adelante se explicará. En línea con lo que acabamos de apuntar sostiene el Grupo de Trabajo respecto a un ordenador o servidor, el carácter técnico no se pierde por al aumento del volumen del número de recursos utilizados, es decir por la presencia de muchos ordenadores o de muchos servidores. Cuestión distinta será la consideración de estos elementos como "medios" de tratamiento y la consiguiente aplicabilidad de la cláusula prevista en el artículo 4.1.c) de la Directiva. La redacción final del RGPD, como luego se verá, hace que este debate tenga mucha más trascendencia del que originalmente pudiera parecer.

Sin embargo, previamente a entrar en el concepto de equipamiento o medios, hay que atender a otro de los términos más complejos: el marco de actividades[490]. Para definir este concepto, el Grupo de Trabajo recurre a tres factores[491]: grado de implicación del establecimiento en las actividades en cuyo marco se traten los datos personales, la naturaleza de las actividades del establecimiento, y, a nuestro juicio el más relevante, que se garantice una protección efectiva a los ciudadanos de una manera sencilla, viable y previsible. Pero además ha añadido recientemente un elemento relevante, con base en la Sentencia TJUE de 13 de mayo de 2014, en el conocido caso Costeja[492]: "actividades indisociablemente ligadas", que conlleva que si en un análisis caso por caso de los hechos hay un vínculo indisociable entre las actividades de un establecimiento en la Unión Europea y el tratamiento de los datos llevados a cabo por un responsable no establecido en la UE, se aplicará a dicho tratamiento por parte de la entidad no europea, con independencia de que el establecimiento europeo desempeñe o no un papel concreto en el tratamiento de los datos. En lo que a nosotros ahora nos ocupa, lo más relevante, es que dicha interpretación confirma la interpretación extensiva del artículo 4.1.a).

---

considera que el centro de datos en Hungría solo está implicado en el mantenimiento técnico. Bien es cierto que en la actualización que mencionamos en la siguiente nota, se utiliza el término "establecimiento húngaro".

[490] Buena prueba de su complejidad es que, a pesar de haber sido tratado en el Dictamen 8/2010 ya citado, el Grupo de Trabajo ha emitido un Dictamen de actualización específico sobre esta materia y que se centra en particular en este concepto. ARTICLE 29 DATA PROTECTION WORKING PARTY. Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain. 16 de diciembre de 2015. Disponible en web: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp179_en_update.pdf

[491] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 8/2010. ob. cit.

[492] Unión Europea. Tribunal de Justicia de la Unión Europea (Gran Sala). Caso Mario Costeja vs. Google (C 131/12). Sentencia de 13 de mayo de 2014.Acceso al texto de la conocida Sentencia en el siguiente enlace: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

Mayor importancia tiene si cabe para el objeto de estas líneas, el concepto de "medios" previsto en el artículo 4.1.c). La importancia para la computación en nube de este criterio es obvia, y buena prueba de ello es que el Grupo de Trabajo ya señalaba que: "Esta disposición presenta especial relevancia a la luz de la evolución de las nuevas tecnologías y, en particular, de Internet, que facilita la recogida y el tratamiento de datos personales a distancia y con independencia de cualquier presencia física del responsable del tratamiento en el territorio de la UE/del EE"[493]. A la hora de definir qué se entiende por medios o por "*equipment"* [494] en la versión inglesa, el Grupo de Trabajo ha optado por una interpretación muy amplia. Y esta no solamente en el ya citado Dictamen 8/2010 en el que habla de "una amplia interpretación del criterio, que, por lo tanto, incluye intermediarios humanos y/o técnicos"[495]; sino que nos encontramos con una línea argumental utilizada también en otros dictámenes con base en la consideración de que el titular de los datos no debe verse sin protección cuando sus datos están siendo tratados en su país solamente porque la organización que lleva a cabo el tratamiento no ha elegido establecerse en su país[496]. Así parece recogerlo el Considerando 20 de la Directiva 95/46 cuando señala 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". Y similares razonamiento y lenguaje se pueden observar en el Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda[497], en el Dictamen 5/2009 sobre las redes sociales en línea[498], o en el Dictamen 13/2011 sobre servicios de geolocalización en dispositivos inteligentes[499]. Más recientemente el Dictamen 8/2014 sobre los recientes

[493] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 8/2010. ob. cit, p. 21.
[494] Nos encontramos ante uno de esos supuestos en el que la terminología plantea dificultades en las traducciones juradas. Así, el Grupo de Trabajo del artículo 29 recordaba que "Cabe señalar que existe una diferencia entre la palabra utilizada en la versión inglesa del artículo 4, apartado 1, letra c), «equipment» y el término utilizado en otras versiones lingüísticas del artículo 4, apartado 1, letra c), «medios», más cercano al término inglés «means». La terminología utilizada en otras versione lingüísticas del artículo 4, apartado1, letra c), es asimismo coherente con el tenor del artículo 2, letra d), en donde se define al responsa", en Dictamen 8/2010. ob. cit. p. 23.
[495] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 8/2010", ob. cit, p. 23.
[496] GRUPO DE TRABAJO DEL ARTÍCULO 29. 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. 30 de mayo de 2002. Disponible en web: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_es.pdf
[497] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda. 4 de abril de 2008. Disponible en web: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_es.pdf
[498] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 5/2009 sobre las redes sociales en línea. 12 de junio de 2009. Disponible en web: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_es.pdf
[499] DATA PROTECTION WORKING PARTY. Opinion 13/2011 on Geolocation services on smart mobile devices". 16 de mayo de 2011. Disponible en web: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf

desarrollos en la Internet de las Cosas señalaba con rotundidad lo siguiente: "De hecho, todos los objetos que son utilizados para recoger y tratar posteriormente datos de las personas en el contexto de la prestación de servicios en la IoT son calificados como "medios" en el sentido de la Directiva. Esta calificación obviamente se aplica a los dispositivos en sí mismos (contadores de pasos, monitoreos de sueño, dispositivos caseros conectados tales como termostatos, alarmas de humo, gafas conectadas o relojes…etc.). También se aplica a los dispositivos terminales de los usuarios (teléfonos inteligentes o tabletas) en los que el software o las aplicaciones han sido previamente instaladas tanto para controlar el entorno del usuario a través de sensores incrustados o interfaces de red, como para enviar los datos recogidas por estos dispositivos a los distintos responsables involucrados"[500]. En fin, la interpretación extensiva también ha sido acogida, lógicamente, por la AEPD, tal y como se puede observar, entre otros, en el Informe Jurídico 314/2008[501] o en el Informe 0454/2009[502], en los que se recoge la doctrina sentada ya en mayo de 2002 por el Grupo de Trabajo en cuanto a la consideración como medios de elementos tales como PCs, terminales o servidores. De hecho, como señala el profesor Van Eecke, la mayoría de las autoridades interpretan el concepto de equipamiento de manera muy amplia[503].

Con base en esta interpretación tan amplia, resulta complejo no considerar que en aquellos casos en que un responsable del tratamiento que se encuentre ubicado en un territorio de un Estado tercero, que recurra a contratar como encargado del tratamiento a un proveedor de servicios en nube, se ve sometido a la normativa comunitaria. Prueba de ello es que como recoge el Grupo de Trabajo del artículo 29 en 2002 y reproduce la AEPD en 2009, "no es

[500] DATA PROTECTION WORKING PARTY Opinion 8/2014 on the on Recent Developments on the Internet of Things. 16 de septiembre de 2014. Disponible en web: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf Menor rotundidad ha tenido la actualización del dictamen 8/2010 emitido por el Grupo de Trabajo en diciembre de 2015 en el que señala que "si bien el TJUE no discute en su Sentencia si el uso de un nombre de dominio nacional y/o de robots para recoger información de sitios web europeos desencadenaría la aplicación de la normativa europea con base en el test del "uso de medios" del artículo 4.1c), la sentencia bajo ningún concepto excluye la posibilidad de que las actividades de los responsables que no tengan establecimiento de ninguna clase en la UE estén sometidos a los requerimientos de protección de datos de la UE". DATA PROTECTION WORKING PARTY. Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain. Ob. Cit. p. 2.

[501] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Informe Jurídico 314/2008. Disponible en web: https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/reglamento_lopd/common/pdfs/2008-0314_Art-ii-culo-3-de-la-RDLOPD.-Responsable-fuera-de-la-UE-encargado-en-Esapa-n-a..pdf

[502] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Informe 0454/2009. Disponible en web: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2009-0454_Aplicaci-oo-n-LOPD-a-tratamiento-de-datos-efectuado-por-una-empresa-no-establecida-en-territorio-espa-n-ol.pdf

[503] VAN EECKE, P. Cloud Computing: Legal Issues. *DLA Pipper*. Disponible en web: http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/DLA_Cloud%20computing%20legal%20issues.pdf

necesario que el responsable del tratamiento tenga un control total sobre los medios, bastando con que determine qué datos se recogen, se almacenan, se transfieren, se modifican, etc., de qué forma y con qué objetivo". Si como posteriormente se razonará, habitualmente el cliente es el responsable porque fija los fines y los medios; si como veremos los fines y los medios suponen la adopción de decisiones como las que acabamos de enumerar; la conclusión lógica es la plena aplicabilidad de la normativa europea correspondiente cuando el proveedor tenga sus medios en territorio de aplicación.

Creemos por tanto, y como conclusión de este punto interpretativo del artículo 4.1.c), que la búsqueda de un supuesto de no aplicabilidad a un proveedor cloud que tenga su centro de datos en territorio UE es solamente posible mediante la construcción de un caso ad hoc. De hecho una cláusula como esta y la interpretación tan amplia que de la misma se realizan, ha recibido críticas por su aplicabilidad a supuestos en que es clara la ausencia de conexión. Así ocurre por ejemplo un responsable no está establecido en territorio de la UE y no trata datos de ciudadanos europeos, pero sí que recurre a equipos ubicados en territorio europeo. Y sin embargo, a pesar de estas interpretaciones materiales tan extensivas, bajo la Directiva quedan fuera supuestos como los de responsables de fuera de la UE que tratan de manera exclusiva o en gran medida con ciudadanos europeos pero que no tienen medios de tratamiento en dicho territorio, ni tampoco los tienen los encargados a los que contratan dicho tratamiento[504].

Procede ahora adentrarse en el RGPD, de momento en lo que concierne al ámbito territorial de aplicación:

"Artículo 3

Ámbito de aplicación territorial

1. El presente Reglamento se aplica al tratamiento de datos personales en el marco de las actividades de un establecimiento del responsable o del encargado del tratamiento en la Unión, con independencia de que el tratamiento tenga lugar en la Unión o no.

[504] ZEITER, A. The New General Data Protection Regulation of the EU and its Impact on IT Companies in the U.S. Transatlantic Technology Law Forum, A joint initiative of Stanford Law School and the University of Vienna School of Law. *TTLF Working Papers.* 2014, nº 20. p. 1-30. (p. 8) *http://law.stanford.edu/wp-content/uploads/2015/07/zeiter_wp20.pdf*

2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que estén en la Unión por parte de un responsable o un encargado del tratamiento no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si se requiere o no un pago por parte del interesado; o

b) el control del comportamiento de su comportamiento siempre que su comportamiento tenga lugar en la Unión Europea.

3. El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable del tratamiento que no esté establecido en la Unión sino en un lugar en que sea de aplicación la legislación nacional de un Estado miembro en virtud del Derecho internacional público".

La combinación de ambos elementos exige un cuidadoso análisis respecto a cuándo resultará aplicable la normativa europea de protección de datos en entornos de computación en nube, condicionante de las líneas que siguen. Vamos a comprobar cómo muchas de las reflexiones utilizadas van a resultar de utilidad, particularmente en el plano conceptual.

La primera de las novedades a destacar es que ya no solamente resulta aplicable la fórmula "en el marco de las actividades de un establecimiento…" al responsable, sino también a un encargado del tratamiento con independencia de dónde se lleve a cabo el tratamiento de los datos. Partiendo de la consideración que luego veremos de que el proveedor de servicios en nube en la mayoría de las ocasiones ostenta la condición de encargado del tratamiento, los debates sostenidos respecto a qué entendemos por marco de actividades y qué entendemos por establecimiento, adquieren una particular relevancia. Mayor importancia reviste si tenemos en cuenta que el criterio que sí se ha eliminado es el concerniente al equipamiento. Por tanto, si estamos ante un responsable no radicado en territorio de la Unión Europea, pero que recurra a un encargado sí incardinado, no bastará con que recurra a equipamiento, sino que será necesario determinar si el encargado tiene o no un establecimiento en un Estado miembro. A este respecto debemos señalar que, en coherencia con lo anteriormente apuntado, la mera existencia de un centro de datos o de una granja de servidores en territorio europeo, no será causa suficiente para considerar aplicable la normativa europea. No estamos hablando en este caso de los datos que pudiera tratar el centro de datos de sus empleados, proveedores o servicios de mantenimiento, respecto de los cuales actúa como

responsable y a los que sí le sería aplicable en cuanto que unidad organizativa el concepto de establecimiento. Aquí nos estamos refiriendo únicamente al ejercicio de una actividad que tiene un componente meramente técnico, de seguimiento de las instrucciones dadas por el responsable y que por tanto, se insiste, no tendría el concepto de establecimiento propiamente dicho. En el marco de la Directiva, esta laguna de aplicabilidad al proveedor se vería superada a través de la cláusula de recurso a los medios en territorio de la UE, pero esta ha desaparecido en el caso del RGPD. Por tanto, a pesar de que en un primer momento la inclusión del encargado en el RGPD pudiera conllevar una ampliación del ámbito de aplicación de la normativa europea, no tiene por qué ser así. Cuestión distinta es que el concepto de establecimiento no deja de ser amplio y por tanto cualquier centro organizativo de naturaleza comercial, publicitaria o de gestión de negocio que tenga una misión hacia terceros que vaya más allá del componente técnico, y que se encuentre radicado en territorio comunitario, conllevará la aplicación al tratamiento de datos. Al margen quedará igualmente lo previsto en el artículo 3.2 que probablemente es el que mayor repercusión tiene dentro de esa suerte de universalización de la normativa europea.

Efectivamente, la principal novedad es que se establece que la normativa europea se aplicará también a los procesamientos de datos de sujetos que estén en territorio UE cuando dicho tratamiento se lleve a cabo por un responsable o un encargado no establecido en la Unión, siempre que las actividades de tratamiento estén relacionadas con el ofrecimiento de bienes y servicios a los interesados en la Unión o el seguimiento de su comportamiento.

Estamos ante una de las previsiones del RGPD más debatidas y comentadas. El Grupo de Trabajo del artículo 29 señaló por su parte la necesidad de clarificar la referencia al ofrecimiento de bienes y servicios con la finalidad de incluir servicios no remunerados, algo que desde su paso por el Parlamento Europeo, como se puede ver más arriba, ha sido admitido. También sugirió la modificación de la redacción del segundo supuesto para que se pudieran incluir los supuestos que conlleven el análisis o predicción de las preferencias personales, comportamientos o actitudes del sujeto aunque no se creen perfiles como tales. De hecho hay quienes sostienen que, de conformidad con el Considerando 21[505] de la propuesta, precisamente el segundo supuesto está vinculado a la creación de perfiles. En

[505] (21) "Para determinar si se puede considerar que una actividad de tratamiento «controla la conducta» de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet con técnicas de tratamiento de datos que consistan en la aplicación de un «perfil» a un individuo con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes".

este sentido el Comisionado de Información británico ha afirmado que, sin perjuicio de que el objetivo que pretende la normativa propuesta es deseable, sin embargo es difícilmente realizable en la práctica, por lo que sugiere que se aplique una fórmula más abierta respecto de los responsables del tratamiento establecidos fuera de la UE . Esta postura sin embargo no coincide con la expresada por otros países como Francia que ha sostenido que incluso se debería cubrir cualquier procesamiento de datos de ciudadanos de la UE, y no solamente cuando se les ofrecen bienes o servicios o esté relacionado con el control de su conducta.

Con esta medida se quiere poner coto a ciertas prácticas de algunos de los grandes actores de Internet (buscadores, redes sociales y demás) quienes, amparándose en su sumisión a las leyes americanas, han tenido poco menos que carta blanca para tratar los datos personales de los europeos. Obviamente este ha sido uno de los aspectos más criticados por el Gobierno americano al señalar que bajo esta propuesta la Unión Europea puede tener jurisdicción sobre una persona que gestiona una Web que de otro modo no tiene ningún vínculo jurídico con Europa y que las no intencionadas consecuencias de esa suerte de barrido jurisdiccional pueden llegar a afectar negativamente a la economía de Internet. De hecho como afirma Anne Zeiter, se puede decir, sin exageración, que para cualquier compañía no europea, esta previsión es probablemente la más importante de todo el Reglamento[506]. Podemos añadir que si bien la eliminación de la cláusula de los medios en el artículo 4.1c) tenía su trascendencia, el campo de actuación con esta previsión es todavía mayor. Resulta difícil pensar en un proveedor de servicios en nube que no ofrezca bienes o servicios a ciudadanos europeos en un servicio que, por naturaleza, tiene una esencia global. Incluso aunque sea una cuestión de matiz, los progresivos cambios del texto han ido ampliando el campo de acción. Durante prácticamente la totalidad de la tramitación se ha hablado de la oferta de bienes y servicios a “residentes”, sin que en el texto final, en línea con lo defendido por el Parlamento Europeo, sea necesaria la concurrencia de dicha residencia y bastando con la presencia en la Unión. Bien es cierto que el impacto fundamental de esta medida para los proveedores vendrá dado no tanto en su condición de encargados de tratamiento, sino en sus muy amplias relaciones con un usuario final, cuyos datos trata para muy diferentes fines. Es decir, será en su condición de responsable del tratamiento cuando para un proveedor de servicios en nube esta previsión tenga un mayor impacto.

[506] ZEITER, A. Ob. cit. p. 9.

Retomando lo que hemos apuntado al principio de este apartado, en realidad con este planteamiento estamos ante uno de los escenarios más complejos a los que el Derecho se enfrenta en Internet cual es el de su naturaleza global, el de la reducción del espacio y del tiempo a lo más insignificante, siendo la reducción de la dimensión espacial particularmente relevante en el entorno de la computación en nube. Internet, casi por definición, implica normas de múltiples jurisdicciones y elementos como el tipo de usuario, la ubicación de los servidores o del ordenador del usuario, o la combinación de estos elementos pueden ser tenidos en cuenta[507]. La pretensión de universalizar la normativa europea busca proteger a sus ciudadanos pero sin duda chocará con disposiciones de otros Estados de fuera de la Unión Europea lo que conllevará un escenario de alta conflictividad política y judicial.

Como conclusión, con base en la actual normativa, la Directiva comunitaria resultará de aplicación siempre que el cliente responsable de los datos se encuentre radicado en territorio del Espacio Económico Europeo o bien el prestador de servicios en nube esté radicado en territorio comunitario; o bien cuando el cliente o el prestador utilicen equipamientos radicados en territorio comunitario, salvo que la finalidad de los mismos sea de mero tránsito.

Conforme al RGPD, este se aplicará cuando el tratamiento se realice en el marco de las actividades de un establecimiento del responsable o del prestador establecidos en la UE, o bien cuando el prestador actúe como responsable ofreciendo sus servicios a interesados en la UE, o bien cuando sea un responsable no prestador quien ofrezca dichos bienes o servicios y contrate como encargado a un proveedor, con independencia de que este no se encuentre radicado en territorio de la UE.

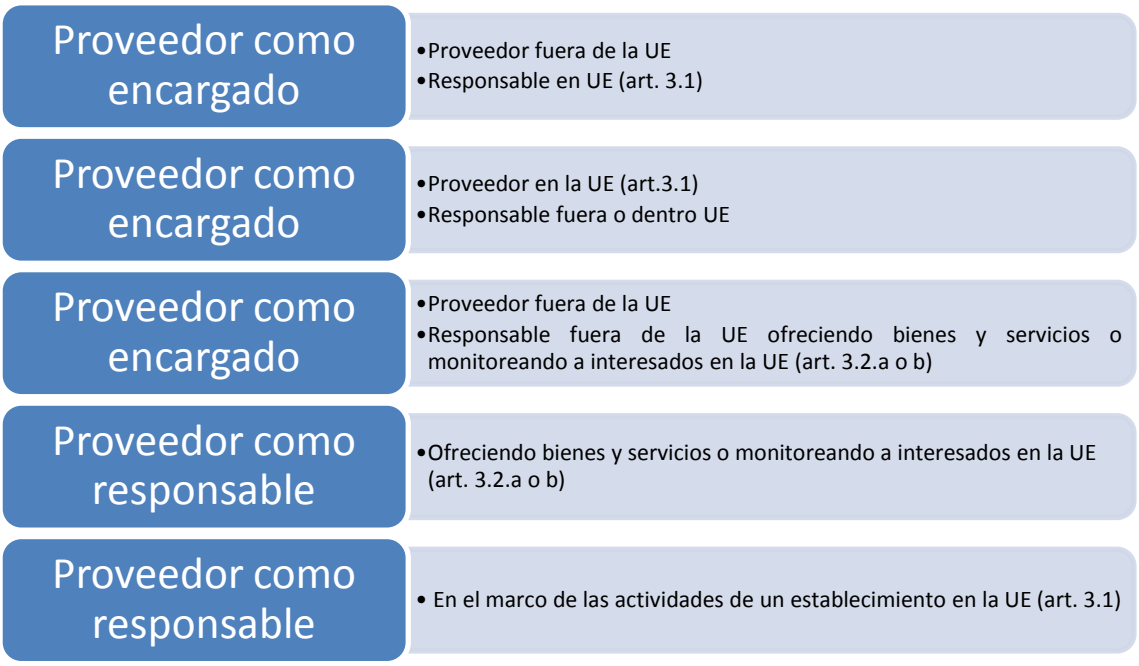
En definitiva, se va a producir una suerte de universalización de la normativa comunitaria, o de paneuropeísmo en términos de Mantelero[508], por cuanto se hace difícil pensar en un prestador de servicios que no ofrezca los mismos a interesados que residan en la Unión. Además la utilización del Reglamento como fuente hace que se trate de una aplicabilidad directa. Utilizando la terminología propia del Derecho Internacional Privado, el hecho de que se recurra a cualquier punto de conexión con la Unión Europea, por mínimo y lejano que este sea, para justificar la aplicación de la normativa europea, va a hacer que resulte difícil encontrar un supuesto en el que aquella quede fuera. Cuestión distinta será la capacidad de

[507] REINGOLD, B., MRAZIK, R. y D'JAEN, M. ob. Cit.
[508] MANTELERO, A. Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution [en línea]. *European Journal for Law and Technolo*gy. 2012. vol. 3, nº. 2. Disponible en web: http://ejlt.org/article/view/96/253

aplicar dicha normativa *de facto*, máxime si ya con la Directiva se plantean problemas en los supuestos cuando los responsables de los datos no tienen presencia física en territorio UE[509].

No cabe por último la posibilidad de disponer de la normativa contractualmente. Este ha sido el criterio fijado por la AEPD y plantea los problemas derivados de la normativa sobre condiciones generales de contratación, la naturaleza de los contratos de adhesión o la protección en definitiva del consumidor[510], cuestiones todas ellas que se tratarán en este mismo capítulo

A través del siguiente gráfico se describen las situaciones posibles de aplicación de la normativa europea con base en el RGPD.



Fuente: elaboración propia

[509] REINGOLD, B., MRAZIK, R. y D'JAEN, M. ob. cit., p. 2,
[510] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía para Clientes que contraten el servicio de cloud computing. ob. cit. p. 13.

2 El estatuto jurídico del prestador de servicios en nube

Uno de los elementos clave de cualquier aproximación jurídica es determinar qué papel juegan los diferentes sujetos que participan de una relación contractual en el ámbito de los contratos en nube y, en particular, el prestador de servicios en nube. Se trata en definitiva de concretar si a este se le debe considerar como un responsable del tratamiento o como un encargado del tratamiento, que son las dos categorías de sujetos participantes que la normativa tradicional de protección de datos ha contemplado. Estamos ante una cuestión fundamental, y ya no solamente por su íntima conexión, como se acaba de ver, con la legislación aplicable[511], sino también a la hora de fijar el trascendental régimen de responsabilidad[512]. No en vano, tanto el régimen jurídico de la Directiva como el de la LOPD son más exigentes con los responsables que con los encargados del tratamiento, al igual que ocurre ahora con el RGPD, aunque este último sin duda ha reforzado el conjunto de obligaciones de los encargados, y basta para ello ver el ya referido art. 3.1.

Se trata de una cuestión que presenta una particular dificultad en el ámbito del *cloud computing* por cuanto la nube puede ser oscura en ocasiones, haciendo difícil para los usuarios visualizar con quién está tratando[513]. Así, el SEPD llega a decir que es un tema particularmente delicado por cuanto la responsabilidad en el tratamiento de los datos puede incluso llegar a evaporarse[514], a ser oscura[515]. En otras latitudes este problema también está presente[516]. Y Vincent y Hart señalan que a diferencia de un servidor fijo en una oficina o en un centro de datos, los datos en la nube pueden potencialmente estar ubicados en cualquier lugar del mundo e incluso en múltiples centros de datos en múltiples copias a lo largo y ancho del mundo. Incluso nos podemos encontrar con que un proveedor pueda no saber dónde están localizados los datos[517]. A nuestro juicio son dos los motivos fundamentales que

---

[511] ARTICLE 29 DATA PROTECTION WORKING PARTY Opinion 8/2010 on applicable law", ob. cit.

[512] La importancia del principio de responsabilidad es una materia nuclear, y buena prueba de ello es el contenido del "Dictamen 3/2010, sobre el principio de responsabilidad. GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 3/2010, sobre el principio de responsabilidad. 13 de julio de 2010. Disponible en web: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_es.pdf

[513] ARTHUR COX. Technology Group Briefing. Cloud Computing & The Law. mayo de 2010. Disponible en web: http://www.arthurcox.com/uploadedFiles/Publications/Publication_List/Arthur%20Cox%20-%20Cloud%20Computing%20and%20the%20Law,%20May%202010.pdf

[514] EUROPEAN DATA PROTECTION SUPERVISOR. Opinion on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe. Ob. Cit. p. 6.

[515] ARTHUR COX. Ob. Cit. p. 2.

[516] Como señala la profesora Gowri Menon en el caso de la India, "puede que no sea siempre fácil distinguir al responsable del tratamiento", MENON, G. Regulatory Issues in Cloud Computing -An Indian Perspective. *Journal of Engineering, Computers & Applied Sciences (JEC&AS)*. July 2013, vol. 2, nº 7. p. 18-22. Diponible en web: http://borjournals.com/a/index.php/jecas/article/viewFile/95/pdf

[517] VINCENT, M. y HART, N. Cloud Computing-Legal Issues in the Cloud. Ob. Cit. p. 3.

explican lo nebulosa que puede resultar esta cuestión: la asimetría que en muchas ocasiones acompaña a este tipo de servicios y que, como se va a ver a lo largo de este capítulo, es un elemento clave a la hora de configurar un adecuado régimen jurídico; y la cadena de subcontrataciones que en muchas ocasiones exige el dinamismo y la elasticidad consustanciales a la prestación del servicio, sobre las cuales el RGPD ha introducido importantes novedades con obligaciones directas para los encargados del tratamiento[518].

La importancia de esta cuestión ha sido recalcada por la Comisión Europea durante el proceso de aprobación del RGPD. Así, señalaba que los problemas definitorios se amplificaban en el contexto del *cloud* y subrayaba que aunque ellos mismos –los prestadores- se consideran como meros encargados[519], sin embargo dependería de las circunstancias[520].

Recordemos en primer lugar las definiciones que de ambos conceptos nos da la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995[521], relativa a la

[518] PATRIKIOS, A. Getting to know the GDPR, Part 2 – Out-of-scope today, in scope in the future. What is caught? [en línea]. *Privacy and Information Law Blog*. 20 de octubre de 2015. Disponible en web: http://privacylawblog.fieldfisher.com/2015/getting-to-know-the-gdpr-part-2-out-of-scope-today-in-scope-in-the-future-what-is-caught

[519] A título de ejemplo ver AMAZON WEB SERVICES. Whitepaper on EU Data Protection. octubre de 2015. p. 10. Disponible en web: https://d0.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper_EN.pdf
En este documento se señala, entre otras cosas, "que como proveedor de una infraestructura *self-service* que está bajo el completo control del cliente, incluyendo lo referido a cómo y si un dato es objeto de tratamiento, AWS solamente facilita los servicios para los clientes que quieren subir y tratar contenido en la red de AWS. En este contexto, AWS no tiene ningún conocimiento de lo que los clientes están subiendo a su red, incluyendo si dicho contenido recoge o no datos personales. Los clientes de AWS pueden también recurrir a la encriptación para convertir el contenido en ininteligible para AWS. AWS no trata contenido del cliente excepto en lo necesario para facilitar os servicios (o para cumplir con la ley o una norma válida e imperativa)". De similar modo, ORACLE. Data Processing Agreement for Oracle Cloud Services. Versión de 31 de julio de 2015. Disponible en web: http://www.oracle.com/us/corporate/contracts/cloud-dpa-2625278.pdf. Afirma que "El cliente seguirá siempre siendo el responsable de los datos para las finalidades del Servicio Cloud, el Acuerdo y este Acuerdo de Tratamiento de Datos".

[520] EUROPEAN COMMISSION. 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. 25 de mayo de 2012. p. 18 del Anexo II. Disponible en web: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf

[521] Al margen dejamos la postura de quienes sostienen que la dualidad responsable/encargado no es susceptible de ser aplicada en entornos de cloud computing. Es el caso del proyecto de investigación de la Queen Mary University que viene a sostener que en muchos casos estos proveedores son meros intermediarios que deberían gozar del estatus propio de estos sujetos recogido en la Directiva de Comercio Electrónico. QUEEN MARY COLLEGE. UNIVERSITIY OF LONDON. Cloud Legal Project. Materiales disponibles en web: http://www.cloudlegal.ccls.qmul.ac.uk/

protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos: es 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.d); mientras que encargado del tratamiento es 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) de la Directiva 95/46); y ello bajo la forma jurídica y con los requisitos de seguridad a los que hace referencia el art. 17 de la Directiva, fundamentalmente en lo concerniente a que la actuación del encargado está sometida exclusivamente a las instrucciones del responsable y a la necesidad de que se regule por contrato u otro acto jurídico, sin perjuicio de que aquel también está vinculado por las medidas de seguridad establecidas por la legislación del Estado miembro en el que esté establecido.

El RGPD, a pesar de la falta de claridad a que en muchas ocasiones ha dado lugar la determinación del estatuto de que gozan las partes, apenas incluye algún añadido y define al responsable en su artículo 4.5 como "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 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"[522]*;* mientras que considera encargado, según su artículo 4.6 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". Así por tanto muchas de las reflexiones que se han venido haciendo y que se harán siguen siendo perfectamente válidas.

[522] Cabe señalar que durante la tramitación del Reglamento, en diferentes fases, la fórmula utilizada era la de fijación de los fines, *condiciones* y medios. Una de las cuestiones a determinar es si el inciso que originariamente añadía la Propuesta de Reglamento, que ya no hablaba solamente de fines y medios para determinar quién es el responsable, sino que hablaba de "fines, condiciones y medios". El añadido de la expresión "condiciones" suponía una novedad con respecto de la Directiva. A dicha novedad le dio una particular importancia el SEPD al afirmar que dicho cambio ponía más énfasis en la responsabilidad de los que determinan cómo se organiza concretamente la actividad de tratamiento de datos y que por ello hablar de corresponsabilidad refleja mejor el nivel subyacente de influencia en las actividades de tratamiento . Sin embargo, la omisión de dicho inciso en la versión final y el mantenimiento por tanto de la expresión fines y medios hace que no proceda profundizar en esta argumentación.

En principio la labor desempeñada por un prestador de servicios en nube es la propia de un encargado del tratamiento y así pareció haberlo asumido la ENISA en su conocido informe de 2009 sobre "*Cloud computing:* beneficios, riesgos y recomendaciones para la seguridad en la información".

	Customer	Provider
Lawfulness of content	Full liability	Intermediary liability with Liability exemptions under the terms of the E-commerce Directive (1) and its interpretation.[1]
Security incidents (including data leakage, use of account to launch an attack)	Responsibility for due diligence for what is under its control according to contractual conditions	Responsibility for due diligence for what is under its control
European Data Protection Law status	Data controller	Data processor (external)

Reparto de responsabilidad ente el cliente y el proveedor de servicios en nube
Fuente: ENISA

En la misma línea se sitúa el ámbito académico que ha opinado sobre la cuestión. Así por ejemplo García Mexía afirma que "con las leyes españolas en la mano, la puesta a disposición de los datos por parte del cliente de nube a favor del proveedor de tales servicios no implica cesión o comunicación en sentido estricto de los mismos, al existir entre proveedor y cliente un contrato de "servicio al responsable" del fichero"[523]. Igualmente Serrera Cobos afirma que esta tecnología se encuadra "…en la figura denominada "acceso a datos por cuenta de terceros"[524], y el proveedor de servicios de Internet asume el rol de "encargado

[523] GARCÍA MEXÍA, P. *Cloud computing*. Sus implicaciones legales. *Revista Aranzadi de derecho y nuevas tecnologías*. 2010, nº 23, p. 79-88.
[524] El artículo 12.1 LOPD define esta figura y dice: "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."

del tratamiento"[525]. Más recientemente Cotino Hueso también lo afirma con rotundidad[526]; mientras que de manera más detallada lo trata Navas Navarro[527]. Mantelero confirma esta postura con base en un triple argumento[528]: primero porque aunque el proveedor mantenga un grado de autonomía y de capacidad de decisión, las tareas y las especificaciones están clara y estrictamente definidas por el usuario a través del contrato; segundo porque solamente el usuario está directamente empoderado por el titular de los datos para tratarlos y el proveedor recibe la información a tratar en interés del usuario; y finalmente porque en esta modalidad de servicios se da gran importancia a los SLA, vinculando a las partes de manera tal que no es posible considerarlos como dos responsables autónomos. Fuera de las fronteras comunitarias, Robert Gellman señala que el prestador de servicios en nube es un "tipo de tercero que mantiene la información sobre, o en nombre de, otra entidad"[529]. Sin embargo, no faltan quienes apuntan que, en la práctica, los servicios en nube a menudo no solo aportan los medios, sino en cierta medida también las finalidades del procesamiento, en cuyo caso se convierten en "responsables del tratamiento"[530].

Desde un punto de vista oficial, el GT del artículo 29 señalaba que "El cliente determina el objetivo último del tratamiento y decide sobre la externalización de este tratamiento y la delegación de la totalidad o de parte de las actividades de tratamiento a una organización externa"[531]. En idéntica línea, la AGPD ha señalado en su Guía para Clientes que contraten el servicio de cloud computing[532] que "quien ofrece la contratación de cloud computing es un prestador de servicios que en la ley de protección de datos tiene la calificación de 'encargado del tratamiento". También la autoridad británica se ha posicionado en favor de dicho estatus,

---

[525] SERRERA COBOS, P. *Cloud Computing* y protección de datos. *Dintel*. 2010. p. 182-184. Disponible en web: http://www.revistadintel.es/Revista/Numeros/Numero9/Normas/serrera.pdf

[526] COTINO HUESO, L. Algunas cuestiones clave de protección de datos en la nube. Hacia una «regulación nebulosa». *Revista Catalana de Derecho Público*. diciembre 2015, nº 51. p. 83-103. Disponible en web: http://revistes.eapc.gencat.cat/index.php/rcdp/article/view/10.2436-20.8030.01.55

[527] NAVAS NAVARRO, S. Computación en la nube: Big Data y protección de datos personales. *InDret* 4/2015. p. 1-48. Disponible en web: http://www.indret.com/pdf/1193_es.pdf

[528] MANTELERO, A. ob. Cit.

[529] GELLMAN, R. Privacy in the Clouds: Risk to Privacy and Confidentiality from Cloud Computing. *World Privacy Forum*. 23 de febrero de 2009. Disponible en web: http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf,

[530] El Grupo de Trabajo del artículo 29 ya reconoció en 2010 que nuevos entornos como los del *cloud computing* plantean dificultades en la distinción clásica entre responsable y encargado del tratamiento. . ARTICLE 29 DATA PROTECTION WORKING GROUP. Opinion 1/2010 on the concepts of "controller" and "processor". febrero de 2010. Disponible en web: http://www.hldataprotection.com/uploads/file/wp169_en.pdf.

[531] ARTICLE 29 DATA PROTECTION WORKING GROUP. Opinion 05/2012 on Cloud Computing. Ob. cit. p. 9.

[532] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía para Clientes que contraten el servicio de cloud computing. Ob. Cit. p. 14.

entrando en un mayor detalle con base en los modelos de nube[533] [534]. La autoridad danesa también ha señalado que un proveedor de nube será en la mayoría de los casos un encargado del tratamiento[535]. Y, como no podía ser de otro modo, los propios proveedores han señalado que en muchos "contextos cloud", los proveedores actúan como encargados del tratamiento[536]. De manera más reciente, la ENISA ha vuelto a subrayar que, lógicamente, el proveedor actúa como un responsable en el caso de proveedores de servicios de correo electrónico, redes sociales o servicios basados en localización[537], es decir, añadimos, cuando se dirige al usuario final cuyos datos recoge; mientras que sin embargo ratifica su posición como encargados en los modelos de implantación tantas veces citados.

Se trata, insistimos, de un elemento clave, puesto que es determinante en toda la legislación del régimen de responsabilidad y en otros muchos aspectos determinantes del régimen jurídico aplicable en materia de protección de datos. Así, el concepto de responsable es determinante, conforme al art. 6.2 de la Directiva, de la responsabilidad en el cumplimiento de los principios de calidad de los datos a que se refiere el apartado 1 del mismo precepto (en la misma línea el artículo 5.2 RGPD); las obligaciones de cumplir con los grandes derechos de acceso, modificación, oposición, cancelación…que recogen los arts. 10 a 12 y 14 de la Directiva son igualmente exigibles ante el responsable (al igual que recoge el

[533] INFORMATION COMMISSIONNER'S OFFICE. Guidance on the use of cloud computing. Disponible en web: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

[534] IOKOMONOU, D. (ENISA). Impact of the proposed data protection regulation on cloud computing. *CSP Forum.* 28 y 29 de abril de 2015. Disponible en web: https://www.cspforum.eu/graphics/2015/speakersfiles/1.%20demosthenes%20Ikonomou_Cloud_DataProtection_CSP2015_DI.pdf

[535] DIGITALISERINGSSTLYRELSEN. Cloud computing and the legal framework- Guidance on legislative requirement and the contractual environment related to cloud computing. 27 de agosto de 2012. Disponible en web: http://digitaliser.dk/resource/2368677

[536] Así lo hacen en el Data Protection Code of Conduct for Cloud Service Providers elaborado por el Cloud Select Industry Group (C-SIG). CLOUD SELECT INDUSTRY GROUP (C-SIG). Data Protection Code of Conduct for Cloud Service Providers. Disponible en web: https://ec.europa.eu/digital-agenda/en/news/data-protection-code-conduct-cloud-service-providers Cabe matizar que inmediatamente señalan que en determinados supuestos podrá ser que actúen como responsables o corresponsables. En concreto señalan que este será el caso cuando el proveedor trate datos personales para sus propios fines, al margen de las instrucciones expresas dadas por los clientes, o estableciendo acciones de marketing directo o publicidad. Además, se añade, en una distinción relevante, el Código está enfocado a las relaciones B2B (cuando el proveedor actúa típicamente como un encargado del tratamiento" para el cliente. Y añade que por tanto quizá no cubra todas las cuestiones que se derivan de unos servicios B2C (cuando el proveedor puede que actúe como un responsable). En la misma línea de atender a la situación concreta para determinar el estatus en ocasiones, ARTHUR COX. Ob. cit. p. 3. Y también, desde el SEPD, Rosa Barceló afirma que probablemente el proveedor es un encargado, pero que dependerá de las circunstancias, en BARCELÓ, R. Cloud Computing: Privacy Risks and EU Policy Considerations. *The Future of Cloud Computing* 26 de enero de 2010. Disponible en web: http://cordis.europa.eu/fp7/ict/ssai/docs/cloudevent-barcelo_en.pdf

[537] En la misma línea GRAHAM, M. y DUTTON, W.H. *Society and the Internet. How Networks of Information and Communication are Changing Our Live*. Oxford University Press 2014. 416 p.

Capítulo III RGPD); las obligaciones sobre notificación y controles previos de los arts. 18 a 21 recaen sobre el responsable y lo mismo cabe decir en cuanto al régimen de responsabilidad por tratamiento ilícito de los datos a que hace referencia el art. 23[538]. No obstante cabe reseñar, como se va a ver a lo largo de este capítulo, que el régimen jurídico aplicable al encargado del tratamiento se ha visto endurecido con el RGPD[539].

Más allá de las definiciones anteriormente señaladas, la computación en nube y otros nuevos retos tecnológicos exigían un esfuerzo en la determinación y el apuntalamiento de lo que debe entenderse por responsable y por encargado que no se ha hecho en el RGPD. El Dictamen 1/2010 del Grupo de Trabajo del artículo 29 (WP 169), es un reflejo del necesario esfuerzo que se debería haber hecho en el plano conceptual.

En la definición de responsable a la que antes hemos hecho mención, el elemento clave es el referido a la determinación de los fines y los medios del tratamiento de los datos. A la finalidad del fichero ya hacía referencia la Convención 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Desde un punto de vista histórico esta Convención define al responsable como cualquier persona que *sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero automatizado* (la cursiva y el subrayado son nuestros). Sin embargo, la Directiva, y por ende también el RGPD, huye de este elemento jurídico y se adentra en elementos fácticos de tal modo que, como señala el GT del artículo 29, el elemento determinante para saber quién es el responsable es preguntar: ¿Por qué está teniendo lugar este tratamiento de datos? y ¿quién lo ha iniciado? Ser el responsable es fundamentalmente la consecuencia primera de la circunstancia fáctica de que una entidad ha decidido tratar esos datos personales para su propio interés. La importancia del elemento fáctico por encima de la designación formal en una norma, en un contrato o en la notificación a la autoridad supervisora, se puso de manifiesto por ejemplo en el caso SWIFT, en el que la sociedad belga aparecía contractualmente designada como encargada del tratamiento de datos y por

[538] ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 1/2010 on the concepts of "controller" and "processor", ob. cit., p. 4. Un buen análisis de dicho documento en TREACY, B. Working Party confirms 'controller' and 'processor' distinction. *Privacy&Data Protection*. Vol. 10, Issue 5. p. 3-5. Disponible en web: https://www.hunton.com/files/Publication/8fe272d1-d29c-4abd-85ae-17843d084da3/Presentation/PublicationAttachment/6d1be60b-be7d-413c-bd6f-6ee37c02c631/Treacy_controller-processor_distinctions.pdf

[539] HON, K. Data protection and service providers - new obligations, liabilities and contract changes loom. *Pinsent Masons*, 7 de septiembre de 2015. Disponible en web: http://www.out-law.com/en/articles/2015/september/data-protection-and-service-providers---new-obligations-liabilities-and-contract-changes-loom/

lo menos en alguna perspectiva de facto era una verdadera responsable de los mismos[540]. El WP 169 lo dice de manera rotunda: "El concepto de responsable del tratamiento es un concepto funcional, destinado a asignar responsabilidades en función de la capacidad de influencia de hecho y, por tanto, está basado en un análisis de hecho más que formal".[541] Reconociendo este dato, el WP 169 señala la necesidad de acudir a aquellas circunstancias –de hecho o de Derecho- de las que habitualmente se puede inferir una capacidad de influencia de hecho, salvo que otros elementos indiquen lo contrario[542]: control emanado de una competencia legal explícita, control emanado de una competencia jurídica implícita o control emanado de una capacidad de influencia de hecho. Lo cierto es que este enfoque de combinación de lo jurídico y de lo fáctico es en cierta medida criticable. Si es necesario, al margen de lo señalado en el contrato, analizar las circunstancias fácticas para determinar quién es responsable y quién encargado, el contrato solamente tiene un componente indiciario o, en categorías jurídicas, sería una suerte de presunción *iuris tantum*. En el ámbito concreto de la computación en nube, nuestra AGPD parece descartar el componente jurídico-contractual, pero también descarta el elemento fáctico. Afirma, con una rotundidad a nuestro juicio excesiva, que "Aunque los contrate con una gran compañía multinacional la responsabilidad no se desplaza al prestador del servicio, ni siquiera incorporando una cláusula en el contrato con esta finalidad"[543].

Como primera conclusión en este punto se puede subrayar que la circunstancia fáctica, de la que el Dictamen da numerosos ejemplos[544], es probablemente la de mayor interés en el análisis de la prestación de servicios en nube. No en vano, cabe la posibilidad de que estemos ante un prestador de este tipo de servicios que acabe siendo un responsable y no un mero encargado, con independencia de cuál sea el contenido contractual establecido. Ello sin perjuicio de que lógicamente el contrato entre proveedor y cliente establece, al menos, una suerte de presunción y por tanto exigirá la carga de la prueba en quienes vean en el

[540] Ver al respecto SAMANI, R., REAVIS, J. y HONAN, B. *CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security*. Elsevier. USA, 2015. 236 p. (p. 142). El caso tuvo tanta relevancia que fue objeto de un Dictamen específico por parte de las autoridades europeas de protección de datos. ARTICLE 29 DATA PROTECTION WORKING GROUP. Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). 22 de noviembre de 2006. Disponible en web: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp128_en.pdf

[541] ARTICLE 29 DATA PROTECTION WORKING GROUP. Opinion 1/2010 on the concepts of "controller" and "processor". ob. cit. p. 10

[542] ARTICLE 29 DATA PROTECTION WORKING GROUP. Opinion 1/2010 on the concepts of "controller" and "processor". ob. cit. p. 11.

[543] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía para clientes que contraten servicios de cloud computing. Ob. cit. p. 13 y 14.

[544] Un buen resumen de los mismos en inglés en TREACY, B. ob. cit. p. 4.

prestador del servicio en nube como responsable de los datos. En este sentido el propio WP 169 apunta que la definición del responsable del tratamiento debe considerarse una disposición jurídica vinculante de la que las partes no pueden desviarse o sustraerse sin más[545].

Estrechando el círculo, la siguiente cuestión por tanto es determinar qué entendemos por el control de los datos o por responsabilidad sobre los mismos. Al respecto disponemos de una interpretación auténtica: el control de los datos se ejerce cuando se determinan los medios y los fines del tratamiento. Así lo ha mantenido también, tal y como se ha transcrito, el RGPD. Se trata en todo caso de dos elementos que no tienen una misma intensidad. La finalidad de los datos es sin lugar a dudas el elemento clave, que trae causa incluso de la citada Convención 108. Los fines para los que se tratan los datos están normalmente vinculados a la actividad de una determinada empresa que ha contratado o externalizado en la nube el tratamiento de los mismos. No parece razonable que una estructura tecnológica basada en la prestación de servicios (SaaS, PaaS, IaaS) participe en la concreción de los fines del tratamiento más allá de lo que se pudiera derivar de un asesoramiento. Los contratos de servicios se caracterizan porque suponen la aportación por una parte de los elementos necesarios para la obtención del resultado solicitado por la otra parte.

Distinta es la cuestión en referencia a los medios, puesto que obviamente la externalización del servicio, concepto que en todo caso a mi juicio no se adapta de manera estricta al concepto de computación en nube[546], conlleva una cierta discrecionalidad técnica por parte del encargado del tratamiento. En este punto el WP 169 ha distinguido dentro del concepto de medios entre los medios técnicos del tratamiento de datos (como por ejemplo qué software y qué hardware pueden usarse) y el "cómo" del tratamiento, que incluye elementos tradicionales del derecho a la protección de datos como la determinación de qué datos pueden tratarse, cuándo deben borrarse los datos o qué terceros pueden tener acceso a los mismos. A juicio del GT del artículo 29, la determinación de los medios sólo implicaría un

[545] ARTICLE 29 DATA PROTECTION WORKING GROUP. Opinion 1/2010 on the concepts of "controller" and "processor". ob. cit. p. 13.

[546] Para una explicación tecnológica de la diferencia entre *Cloud Computing* y *IT outsourcing* ver YIGIBASIOGLU, O.M., MACKENZIE, K. y LOW, R. Cloud Computing: How does it differ from IT outsourcing and what are the implications for practice and research? *The International Journal of Digital Accounting Research*. 2013. nº 13. p. 99-121. Disponible en web: http://www.uhu.es/ijdar/10.4192/1577-8517-v13_4.pdf
En la misma línea pero desde una vertiente más jurídica, CHANG, H. Data Protection Regulation and Cloud Computing. en CHEUNG, A.S.Y. y WEBER, R.H. (eds). *Privacy and legal issues in Cloud Computing.* Edward Elgar Publishing. 2015. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2610615
También en España, cfr. NAVAS NAVARRO. S. ob. cit. p. 5 y siguientes.

control (y consiguientemente, añadimos, la condición de corresponsable) si afectara a elementos esenciales de los medios[547]. En el mismo sentido, Navas Navarro afirma que la actuación por cuenta del responsable "no impide que el encargado tenga autonomía para determinar qué medios técnicos son los más adecuados para mejor servir el encargo que se le ha encomendado".[548]

Esta distinción puede constituir un elemento esencial en la tecnología de la computación en nube a efectos de la determinación del estatuto jurídico de las partes y consiguientemente del régimen jurídico aplicable. Si el prestador de servicios en nube únicamente adopta las soluciones tecnológicas en sentido estricto entonces, a nuestro juicio, sí que cabría hablar de un mero encargado del tratamiento. En la misma línea, la autoridad británica de protección de datos señalaba que "a pesar de que el proveedor facilita una amplia gama de servicios y utiliza un amplio abanico de su propio *expertise* técnico para hacerlo, es simplemente un encargado del tratamiento"[549]. Desde el punto de vista académico, y apoyándose en gran medida en la opinión vertida por el Grupo de Trabajo del artículo 29, se sitúan en la misma opinión Gutwirth, Poullet, de Hert y Leenes[550]. Se subraya por tanto a modo de conclusión que si el prestador de servicios en nube lleva a cabo cualquier determinación respecto a aspectos esenciales del tratamiento de los datos, adquirirá la condición de corresponsable. Si su aportación en cuanto a los medios se limita a lo meramente técnico, la condición de encargado es la única que puede ostentar.

La normativa española, si adoptamos una interpretación estricta de la misma, todavía plantea una mayor complejidad, puesto que la definición del responsable del tratamiento no coincide en su literalidad con la de la Directiva comunitaria ni con la recogida en el RGPD. La Directiva, recordemos, define al responsable como el que determina los fines y los medios del tratamiento de datos personales; mientras que en el caso de la LOPD se define como el que decide sobre la "finalidad, contenido y uso del tratamiento": La diferencia básica radica en que no se hace una específica mención a los medios, sino al contenido y al uso. Solamente

[547] ARTICLE 29 DATA PROTECTION WORKING GROUP. Opinion 1/2010 on the concepts of "controller" and "processor". ob. cit. p. 13. p. 15.
[548] NAVAS NAVARRO, S. ob. cit. p. 21.
[549] INFORMATION COMMISSIONER'S OFFICE. Data controllers and data processors: what the difference is and what the governance implications are. 6 de mayo de 2014. p. 14. Disponible en web: https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf
[550] GUTWIRTH, S. POULLET, Y. HERT, P. y LEENES R. *Computers, Privacy and Data Protection: an Element of Choice.* Springer. 2011. 482 p. (p. 386 y 387)

si interpretamos de manera equivalente dicho concepto al de contenido y uso entonces la doctrina anteriormente expuesta resulta válida. La AEPD no se pronuncia sobre dicha equiparación desde el punto de vista jurídico, pero la doctrina resulta plenamente aplicable si tenemos en cuenta que habla de que "lo importante para delimitar los conceptos de responsable y encargado del tratamiento no resultan ser la causa que motiva el tratamiento de los mismos, sino la esfera de dirección, control u ordenación que el responsable pueda ejercer sobre el tratamiento de los datos de carácter personal que obran en su poder en virtud de aquella causa y que estaría enteramente vedado al encargado del tratamiento"[551].

Uno de los componentes de mayor relevancia dentro de dichos medios es la concreción de las medidas de seguridad, que siempre han gozado de una particular relevancia, incrementada por cierto en el seno del RGPD. Sobre esta cuestión también se ha pronunciado en su Dictamen el GT del artículo 29 señalando que en algunos sistemas jurídicos las decisiones adoptadas sobre medidas de seguridad son particularmente importantes puesto que tales medidas se consideran explícitamente una característica esencial que ha de definir el responsable del tratamiento. Esto plantea la cuestión de qué decisiones en materia de seguridad determinan la condición de responsable del tratamiento en el caso de una empresa a la que se haya externalizado el tratamiento. La lógica, partiendo además de que en determinadas ocasiones nos encontramos en un contexto asimétrico, es que el responsable del fichero indique el nivel de seguridad aplicable dentro de los parámetros exigidos por la normativa (alto, medio y básico en el caso español), lo que permite por tanto una descripción general de las medidas técnicas y organizativas, en palabras del artículo 28.2 RGPD. Basta atender a los parámetros genéricos previstos en los artículos 89 y siguientes del ROPD y su inclusión en el correspondiente contrato (sea en formato bilateral o de adhesión a través de términos y condiciones de uso) para entender cumplimentado el trámite en cuanto que responsable. Estamos hablando de conceptos como el de registro de incidencias, responsable de seguridad, auditorías…etc, ¿qué le corresponderá entonces determinar al encargado sin perder la condición de tal? Todo lo que concierna a los aspectos técnicos y organizativos que desarrollen dichos términos generales. Entenderlo de otra manera llevaría la norma al absurdo en cuanto a pretender que quien recurre a un servicio

[551] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Informe AEPD 287/2006. FATÁS, J.M. y GARCÍA SANZ, F.J. Comentario al art. 5 del Reglamento de desarrollo de la LO 15/1999, de Protección de Datos de Carácter Personal. *Estudios y Comentarios Legislativos (Civitas)*. Editorial Aranzadi, SA, diciembre de 2008. Acceso al referido informe de la AEPD en el siguiente enlace: https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2006-0287_Delimitaci-oo-n-del-responsable-del-fichero-y-del-encargado-del-tratamiento.pdf

tecnológico que se externaliza, valga la expresión, tuviera que fijarle los aspectos técnicos a la empresa especializada en la prestación de los servicios. Recurriendo a un ejemplo, al responsable le corresponderá asegurarse de que el encargado dispone de un sistema para restablecer la disponibilidad y el acceso a los datos, en el caso de un incidente técnico o físico (en palabras del RGPD, artículo 30), pero lógicamente será el encargado el que fije las características técnicas de dicho sistema.

En conclusión, sí además del responsable, el prestador de servicios en nube participa de la fijación de los fines o, como se puede dar en más casos, de los medios en sentido estricto, entonces nos encontraremos ante un supuesto de corresponsabilidad. Y es que efectivamente, otra vía intermedia de la que cabe hablar es la referida a la posibilidad de que exista una responsabilidad conjunta de los datos. Como refleja el Dictamen 1/2010 ya citado, "debido a la variedad de soluciones posibles no puede establecerse una lista o categorización exhaustiva y cerrada de los distintos tipos de control conjunto[552]. Esta situación hace que todavía adquieran una relevancia mayor, si cabe, las cláusulas contractuales que determinen la relación entre el cliente y el prestador de servicios en nube, cuestión a la que atenderemos con posterioridad. Siguiendo la línea con la que venimos trabajando, es digno de mención el hecho de que la LOPD no contemplaba la posibilidad de la responsabilidad conjunta en la definición del responsable del fichero o tratamiento, aunque sí el ROPD. En este sentido sí que resulta digna de elogio la figura de la corresponsabilidad que ha introducido el artículo 24 RGPD cuando dos o más responsables conjuntamente determinen los fines y los medios del tratamiento. Es decir, si de los elementos fácticos a los que hemos hecho mención se observara una participación del prestador de servicios en nube en la determinación de los fines o de elementos esenciales de los medios de tratamiento, entonces cabría la posibilidad de que ambos ostentaran la condición de responsable/cliente y de responsable/prestador de servicios en nube. De hecho, a esta postura parece inclinarse también en alguna medida la autoridad francesa de protección de datos cuando tras afirmar que cuando un cliente utiliza un proveedor está generalmente aceptado que este es el encargado, en determinados casos de PaaS o SaaS públicos los clientes, a pesar de ser responsables por la elección de sus proveedores, no pueden en realidad darles instrucciones y no están en posición de controlar la efectividad de las garantías de confidencialidad y

[552] ARTICLE 29 DATA PROTECTION WORKING GROUP. Opinion 1/2010 on the concepts of "controller" and "processor". febrero de 2010. Ob. Cit. p. 20 y ss, donde se recogen numerosos supuestos de control conjunto.

seguridad; debido principalmente a las ofertas estandarizadas que no pueden ser modificadas por los clientes que no permiten posibilidad alguna de negociación[553].
Como se ha apuntado, también el SEPD considera que el análisis varía en función del modelo de implantación ante el que estemos[554].

- En las soluciones IaaS el cliente (habitualmente una empresa) podría tener una cierta influencia en la determinación de los términos y condiciones del servicio, aunque podría no estar en una posición para negociar las medidas de seguridad. Ahora bien, seguirá siendo responsable respecto a los tratamientos de datos de sus empleados, puesto que le corresponde elegir los medios y condiciones y determinar los fines del tratamiento por parte del proveedor. Al final se remite a que deberá ser establecido claramente en el contrato.
- En las soluciones SaaS el cliente habitualmente no tiene posibilidad de influir en el tipo de servicio ofrecido y puede que su relación no implique ningún tipo de negociación sino un simple sistema de registro, por lo que su control de las operaciones de tratamiento puede ser muy limitado en cuyo caso considera que el principio de corresponsabilidad es más ajustado.

El análisis que el SEPD realiza en este punto merece una crítica por nuestra parte. En primer lugar por cuanto al utilizar el enfoque de los modelos de implantación, no lo está completando ya que no recoge el supuesto de PaaS que, aunque de manera más limitada, también conlleva tratamiento de datos. Por otro lado, las soluciones a las que llega, a pesar de su previo análisis, son demasiado simplistas. Por ejemplo se señala que en el modelo IaaS el cliente tiene una cierta capacidad de influencia, cosa que no ocurre en el modelo SaaS. A nuestro juicio este esquema no responde a la realidad y consiguientemente sus conclusiones son aventuradas. La realidad es que la capacidad de negociación contractual, del SLA o de los términos y condiciones de uso no viene tanto por el modelo de implantación, tampoco por la estandarización del producto (muy propio del software y que podrá conllevar un mayor

[553] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL). Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing. 2012. Disponible en web ; http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf
[554] EUROPEAN DATA PROTECTION SUPERVISOR. Opinion on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe". Ob. Cit. p. 13 y 14.

coste en su caso) sino por el "tamaño" de las partes. En definitiva por su *capacidad* de negociación.

En conexión con anterior, tampoco cabe compartir la postura de la autoridad francesa. La ausencia de capacidad de negociación y la muy generalizada existencia de cláusulas de servicio estandarizadas puede ser causa para determinadas medidas normativas como luego se señalará, pero no es causa en sí misma para un desplazamiento de la responsabilidad, ni para el cambio de estatuto jurídico. En este sentido la Guía elaborada por la AEPD al respecto en el año 2013[555] resulta muy rotunda en cuanto al estatus del cliente de la nube al considerarlo como el responsable del tratamiento, sin que quepa posibilidad alguna de llevar a cabo una modificación de dicho rol a través de las cláusulas contractuales y ello con independencia del tamaño que se pueda tener. En idéntico sentido, el GT del artículo 29 señalaba que "el desequilibrio en cuanto al poder contractual entre un pequeño responsable del tratamiento y un gran proveedor de servicios no debería considerarse una justificación para que el primero acepte cláusulas y condiciones de contratos que no se ajusten a la legislación en materia de protección de datos".

En íntima conexión con el concepto de responsable se encuentra lógicamente el concepto de encargado del tratamiento, cuya determinación y concreción ayuda también a la delimitación que venimos haciendo. La característica esencial es que se trata de un sujeto que actúa por cuenta del responsable lo que conlleva, en línea con lo que acabamos de decir, que está vinculado por los fines del tratamiento y por los elementos esenciales de los medios utilizados para dicho tratamiento; sin perjuicio de que tenga una cierta capacidad de actuación. Así viene en ratificarlo el WP 169 "la delegación aún puede implicar un cierto grado de discrecionalidad sobre cómo servir mejor los intereses del responsable del tratamiento, permitiendo que el encargado del tratamiento elija los medios técnicos y de organización más adecuado"[556], con el límite, más arriba descrito, de que no afecte a elementos esenciales de dichos medios.

Lo cierto es que las características del *cloud computing* hacen que sea difícil en determinadas ocasiones considerar al proveedor como un mero encargado del tratamiento. Como ha señalado el Supervisor Europeo de Protección de Datos siguiendo la referida Opinión del Grupo de Trabajo del artículo 29, aunque en la mayoría de los casos el prestador de servicios

[555] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Ob. cit. p. 13 y 14.
[556] *Idem*, p. 28

en nube va a actuar como un encargado del tratamiento, en determinadas ocasiones puede actuar como un corresponsable o como un responsable del tratamiento en sí mismo, como por ejemplo cuando trate datos para sus propios fines o bien en aquellas ocasiones en que ofrezca sus servicios al usuario final en el marco de relaciones B2C.

La realidad sin embargo de lo que ya se ha descrito es que en la mayoría de los supuestos el proveedor es un simple encargado del tratamiento. Desde el punto de vista formal, la relación entre encargado y responsable ha de ser reflejada en un instrumento, sea un contrato u otro acto jurídico, que quedará por escrito (artículo 17.3 de la Directiva y artículos 26.2.e) y 26.4 RGPD). La realidad es que muchos aspectos técnicos y organizativos que implica el tratamiento serán determinados por el propio encargado, sin perjuicio de que el responsable, en caso de tener capacidad negociadora, pueda fijar las líneas generales o estandarizadas. Además variará en función de ante qué tipo de nube nos encontremos, tanto en lo que concierne al modelo de implantación como al servicio que se esté prestando. No parece que sea lo mismo un acuerdo de prestación de servicio al que se haya llegado con una gran empresa que ha encargado una nube privada, donde parece que el reparto de responsabilidades puede quedar de manera tasada; que en aquellos casos en que una PYME se adhiera a los términos y condiciones de uso establecidos por un prestador de servicios en nube. En este segundo caso estamos ante un ejemplo claro de cláusulas de adhesión en el que la capacidad de negociación es nula (*take it or leave it*) En definitiva como ha señalado la ENISA la determinación del estatutos de responsable o de encargado del tratamiento en el entorno de la nube todavía necesita ser determinado caso por caso y en relación a la naturaleza de los servicios prestados"[557]. En la misma línea apunta la doctrina, y así se señala generalmente cuando el cliente es una gran compañía, el contrato de servicios puede ser personalizado, buscando la consecución de objetivos y fines específicos, lo que no ocurre cuando el cliente es una persona física o un pequeño negocio[558].

En ambos supuestos habrá que ir a aquello que quede reflejado por escrito. No obstante desde el punto de vista jurídico corresponderá a las autoridades de control y a los tribunales en su caso determinar si, con independencia de las características del contrato, las decisiones adoptadas por el prestador de servicios en nube afectan a la determinación de

[557] Tomado de UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. Privacy in the Cloud Computing. Mayo de 2012. Ob. Cit. p. 7. Disponible en web: http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf

[558] ROHRMANN, C.A. y ROCHA CUNHA, J.F.S., Some legal aspects of Cloud Computing Contracts. *Journal of International Commercial Law and Technology.* 2015, vol. 10, nº. 1. p. 37-45. (págs. 40 y 41).

los fines y medios del tratamiento, en cuyo caso el encargado pudiera acabar siendo considerado un responsable del tratamiento (artículo 26.4 RGPD). Si tal fuera el caso, son las partes las que deberían pactar, conforme al artículo 24 RGPD, la división de responsabilidades. Sin embargo, en el supuesto que hemos mencionado de adhesión a unos términos y condiciones de uso ese elemento paccionado no es factible, por lo que habrá que ir caso por caso a observar el correspondiente reparto. Esta cuestión será objeto de desarrollo posteriormente al atender el contrato de prestación de servicios en nube que ha de ser suscrito entre uno y otro.

El panorama por tanto es sumamente complejo. A la vista de lo apuntado la conclusión a la que podemos llegar es que en un principio puede resultar válido el esquema de considerar que será el cliente de la nube el que señale los medios y los fines del tratamiento siempre y cuando se trate de un contrato *ad hoc* firmado entre la empresa/cliente y el proveedor. En todo caso con independencia de los términos en que por escrito se haya procedido a la distribución de responsabilidad entre una y otra parte, ello únicamente conllevará un principio de prueba, sin que sea determinante del análisis que en su caso las autoridades de control o los tribunales pudieran realizar. En estos casos por tanto lo oportuno es partir de la consideración, con independencia del modelo de implantación, de que el esquema será el clásico de considerar como responsable del tratamiento al cliente y de encargado del mismo al proveedor de servicios en nube. Resulta lógico y consustancial a las propias características de la provisión de servicios en nube, que la personalización o adaptación a los requisitos, particularmente en materia de aspectos técnicos de seguridad y tratamiento, no puede hacerse a las características y detalles exigidos por parte de cada cliente. Y es en aplicación de esa lógica en la que bastará con una notificación de aquellas modificaciones más sustanciales o relevantes para entender que el encargad pierda su condición de tal[559].

En aras sin embargo de un esquema de mayor confidencialidad y garantía del sistema y sobre todo de mayor justicia material, en los supuestos en que el mecanismo contractual responda a la naturaleza de contrato de adhesión, sea en su vertiente de términos y condiciones de uso o de acuerdo de nivel de servicio, lo cierto es que la intervención administrativa se hace necesaria. Cuando no existe capacidad de negociación se debería articular un mecanismo de garantía. La primera medida es la de partir del principio de corresponsabilidad cuando quien contratara fuera una PYME. En el caso de este tipo de

[559] DETERMANN, L. *Field Guide to Data Privacy Law*. Edward Elgar. 2nd ed. Cheltenham (UK), Northampton, MA, (USA). 2015. 232 p.

sujetos se hace difícil pensar que un proveedor de servicios en nube no tenga una participación esencial en la determinación, al menos, de las medidas de seguridad para la protección de los datos y de las operaciones de tratamiento de los mismos. Sin embargo sí se estableciera este sistema, se estaría llevando a cabo un planteamiento injusto y contradictorio con lo anteriormente descrito y por ello se hace necesario recurrir a otro instrumento. Así, el segundo de los mecanismos sería el establecimiento de una suerte de *Registros de condiciones contractuales* que estuviera certificado o avalado por la autoridad de control correspondiente en cada país. Esa situación conllevaría que sí se pudiera mantener el esquema clásico en su caso de distribución de responsabilidad. El sistema de registro debería tener una naturaleza voluntaria pero permitiría una garantía de adecuación a la regulación. Los mecanismos de certificación o las cláusulas tipo se están generalizando y otorgan un sello de confianza a quien contrata este tipo de servicios, particularmente de nubes públicas. En este sentido parece haberse posicionado la Comisión Europea[560] y también el Supervisor Europeo de Protección de Datos con base en el habitual desequilibrio significativo en los poderes de negociación entre los proveedores y los clientes. Las vías de certificaciones y códigos de conducta que desarrollaremos en otro punto de este capítulo, en cuanto que mecanismos introducidos por el RGPD, pueden ayudar a la consecución de estos objetivos. Máxime cuando aquellos recogen la necesidad de atender a las particulares necesidades de las PYMES y de las microempresas (artículo 38.1 *in fine* en el caso de los Códigos de Conducta y 39.1 *in fine* para los mecanismos de certificación. Posteriormente, se insiste, por ser consustancial al propio mecanismo de contratación de la nube, volveremos sobre esta idea, que resulta trasladable a otros ámbitos.

Por tanto, con base en el panorama legal actual probablemente no quepa otra opción que la de seguir considerando al prestador de servicios en nube como un encargado del tratamiento. Ello no debe obstar, insisto, a la articulación de mecanismos oportunos a través de los cuales se garantice que la falta de equilibrio en la negociación impida cláusulas abusivas, exenciones de responsabilidad injustificadas y que se haga realidad una de las obligaciones que han de asumir las autoridades nacionales de protección de datos. Establecer una suerte de control previo a través del citado mecanismo de Registro puede ser

[560] EUROPEAN COMMISSION. Commission Staff Working Document, Accompanying the document Communication from the Commisssion to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Unleashing the Potential of Cloud Computing in Europe. Ob. cit. p. 32. Habla del desarrollo de modelos contractuales para los SLA. También desde el punto de vista académico en FELICI, M. y FERNÁNDEZ GAGO, C. (eds). *Accountability and Security in the Cloud*. Springer. 2015. 306 p. (p. 14)

una medida adecuada. El trasfondo de encontrarnos en último término ante un derecho fundamental como el de la protección de datos, puede ser causa suficiente para justificar un mecanismo de este tipo que refuerza las garantías a través de un instrumento de transparencia. Estamos hablando además de un mecanismo voluntario y que en el caso de cláusulas estandarizadas, no supone una carga administrativa desproporcionada para el proveedor[561]. Más adelante se verán los términos y condiciones de los códigos de conducta y de los sistemas de certificación como alternativas a esta propuesta planteada.

Esquema de conclusión con base en el RGPD

Sujeto	Funciones	Estatuto jurídico
Proveedor de servicios en nube	Oferta de servicios a un responsable y fijación de medidas técnicas	Encargado del tratamiento
Proveedor de servicios en nube	Oferta de servicios a consumidor final (servicios de mail, almacenamiento, software…)	Responsable del tratamiento
Proveedor de servicios en nube	Oferta de servicios a consumidor final (servicios de mail, almacenamiento, software…) y uso por este de datos de tercero	Encargado del tratamiento, salvo aplicación de excepción doméstica[562]

[561] En este sentido resulta loable, no solamente en esta vertiente de la determinación del estatuto de los sujetos partícipes, sino en general en cuanto a la falta de equilibrio, el borrador de Código de Conducta para los Proveedores de Servicios Cloud que se ha elaborado partiendo de la consideración de estos como encargados del tratamiento. Ver C-SIG SUB-GROUP ON THE DATA PROTECTION CODE OF CONDUCT. Data Protection. Code of Conduct for Cloud Service Providers. Disponible en web: https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-code-conduct

[562] Desde el punto de vista material, el SEPD llamó en su momento la atención sobre la aplicabilidad de la denominada excepción doméstica con base en la Propuesta de Reglamento de protección de datos. En concreto apela al considerando 15 para subrayar la no aplicabilidad al proveedor de servicios en nube cuando sus medios son utilizados por un consumidor que sí actúa conforme a la referida excepción doméstica y ello porque además de aportar los medios lo hace con fines comerciales. En definitiva cualquier utilización de un sistema de almacenamiento de datos por parte de un particular en el ejercicio de una actividad personalísima para la cual utilice servicios de almacenamiento en nube (una de las prácticas más frecuentes por parte de un particular) conlleva que el prestador de servicios en nube, con independencia del lugar donde radique su establecimiento y donde se procesen los datos, va a estar sometido a la normativa comunitaria. Precisamente la universalización de la normativa europea de protección de datos ha generado un considerable debate.

Proveedor de servicios en nube	Oferta de servicios a un responsable y fijación de fines y medios esenciales	Corresponsable del tratamiento
Proveedor de servicios en nube	Oferta de servicios a un responsable y uso de datos para fines propios (elaboración de perfiles, publicidad…)	Corresponsable del tratamiento
Proveedor de servicios en nube	Oferta de servicios a un responsable y tratamiento de datos de proveedores, empleados o de los propios clientes…etc.	Encargado del tratamiento en el primer caso y responsable del tratamiento en el segundo

Fuente: elaboración propia

Por tanto, y como respuesta en este punto a nuestro objeto general de investigación, podemos afirmar que las categorías jurídico-subjetivas tradicionales de responsable y encargado del tratamiento son perfectamente encajables en el régimen jurídico de la computación en nube. La asimetría tan característica en el entorno del *cloud computing* no conlleva *per se* un desbordamiento de esta parte del régimen jurídico vigente en materia de protección de datos

3 El contrato entre el responsable-cliente y el encargado-proveedor

3.1 Introducción

El elemento contractual es un elemento clave en este tipo de servicios. Estamos partiendo de una consideración general del contrato que consiguientemente deberá reunir todos los requisitos de este instrumento jurídico, sin perjuicio de que descenderemos lógicamente con mayor detalle a uno de los aspectos más relevantes del mismo, el referido a la protección de datos. Este constituye sin duda el aspecto normativo más citado en los términos y condiciones de uso establecidos por los proveedores cloud, particularmente en lo que concierne a la ubicación y confidencialidad de los datos, seguido de las transferencias

internacionales y el papel de los subencargados[563]. Siguiendo la línea de investigación, el objeto final de este apartado es analizar las exigencias que la normativa actual establece para la forma y el contenido del contrato entre encargado y responsable, para ver si se compadecen con las características que exige el *cloud computing*.

Partiendo de la consideración ya sentada de que en la mayoría de las ocasiones el proveedor que ofrece los servicios en nube es el encargado y el cliente el responsable, es necesario que dicha relación se canalice a través de un instrumento jurídico. Así lo contempla la Directiva 95/46 en su artículo 17.3 donde señala que "La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento". En el caso de la normativa española, el artículo 12.2 LOPD recoge que "La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente 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". Por su parte el artículo 26.2 RGPD establece que "el tratamiento por un encargado se regirá por un contrato u otro instrumento jurídico bajo la normativa europea o del Estado miembro…". Analicemos por tanto este contrato o instrumento jurídico desde sus diversas perspectivas: formal, naturaleza y, en especial, su contenido obligatorio y potencial, deteniéndonos en el aspecto específico de la privacidad.

3.2 La perspectiva formal

En primer lugar, desde el punto de vista formal, la normativa europea, la Directiva, no exige que el contrato tenga lugar por escrito, aunque su artículo 17.4 señala que "a efectos de conservación de la prueba, las partes del contrato o del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas de seguridad sí que constarán por escrito o en otra forma equivalente". Cabe puntualizar en palabras de la Audiencia Nacional –en la importante Sentencia de 15 de noviembre de 2002[564]- que "la constancia escrita…se deriva

[563] HON, K., MILLARD, C. y WALDEN, I. Negotiating Cloud Contracts: looking t clouds from both sides now. *Stanford Technology Law Review.* Fall 2012. Vol. 16. Nº 1. p. 79-129. En este artículo se ofrece un abundante estudio comparativo de las condiciones establecidas por diferentes proveedores cloud.

[564] España. Audiencia Nacional (Sección Primera. Sala de lo Contencioso-Administrativo). Sentencia 6324/2002, de 15 de noviembre de 2002. Acceso al texto de la Sentencia en el siguiente enlace:

del contenido del art. 17.3 de la Directiva 95/46/CE donde se establece que la «realización de tratamiento por encargo deberá estar regulada por un contrato o acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento», precepto que la doctrina interpreta en el sentido de que es preciso un contrato escrito". En otra línea argumental, aunque vinculada con lo anterior, la necesidad de que sea por escrito o en cualquier otra forma que permita acreditar la celebración es consecuencia, según recoge la Sentencia del Tribunal Supremo de 17 de abril de 2007[565], de que es necesaria una "una forma que refleje y deje constancia no sólo de su celebración sino de su contenido, que incluso se especifica en sus cláusulas imprescindibles en el propio precepto". De similar modo, la autoridad británica de protección de datos subraya que la constancia escrita implica que el proveedor no podrá modificar las condiciones de las operaciones de tratamiento de datos durante la vida del contrato sin el conocimiento y acuerdo del cliente[566].

En todo caso, se esté o no de acuerdo con ambas interpretaciones –su derivación del apartado 3 o 4 del artículo 17-, la forma escrita será lo habitual por el carácter a distancia de la prestación de este tipo de servicios. Además, en nuestro caso, así lo exige la normativa española, a pesar de que, en general, podemos afirmar que nuestro ordenamiento no es excesivamente formalista (arts. 1278 del Código Civil y 54 del Código de Comercio). Bien es cierto que, como apuntan Orozco Pardo y Moreno Navarrete, existe una tendencia a aumentar el formalismo "como instrumento al servicio de la seguridad jurídica…y como medio para asegurar el respeto a los valores del sistema: buena fe, equilibrio contractual, lealtad en la ejecución, etc."[567]. A mayor abundamiento, el debate se ve superado en el plano comunitario por la previsión del art. 26 RGPD en cuyo apartado 3 se dice que "El contrato o acto jurídico al que se refieren los párrafos 2 (responsable/encargado) y 2a (encargado/subencargado) deberán constar por escrito, incluyendo el formato electrónico".

En numerosas ocasiones –particularmente en los supuestos en que se lleva a cabo entre una PYME y un gran proveedor– esa relación contractual se realiza a distancia, es decir,

---

http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=2956896&links=&optimize=20031128&publicinterface=true

[565] España. Tribunal Supremo (Sección Sexta de la Sala Tercera de lo Contncioso-Administrativo). Sentencia 2778/2007, de 17 de abril de 2007. Acceso al texto de la Sentencia en el siguiente enlace: http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=503664&links=&optimize=20070531&publicinterface=true

[566] INFORMATION COMMISSIONNER'S OFFICE (ICO). Guidance on the use of cloud computing. ob. cit. p. 12.

[567] OROZCO PARDO G. y MORENO NAVARRETE, M.A. El contrato en el contexto de la unificación del Derecho Privado. *Anales del Derecho.* 2011, nº 29. p. 115-160.

mediante la adhesión a los correspondientes términos y condiciones de uso. En este último supuesto será necesario tener en cuenta las previsiones de la Directiva de Comercio Electrónico (arts. 9 y siguientes) y de la LSSI (arts. 23 y siguientes), y cumplir los requisitos formales, y en particular de información, que allí se contemplan. En este sentido, será oportuno dejar constancia si la forma escrita vendrá dada por un documento físico como tal o por ejemplo a través de un documento PDF firmado electrónicamente accesible y susceptible de archivarse[568]; previsión esta última que, como acabamos de recoger, contempla expresamente el RGPD.

3.3 Naturaleza del contrato.

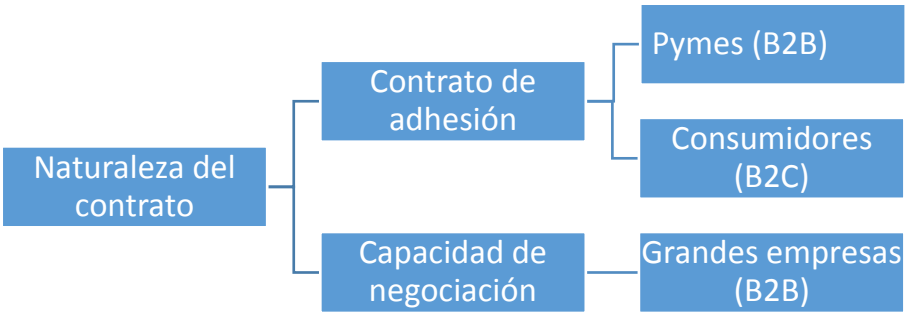
En lo concerniente a la naturaleza del contrato nos podemos encontrar ante un contrato de negociación o ante un contrato de adhesión[569]. Como su propia denominación indica, en el primero el contenido del contrato está paccionado entre las partes del mismo, mientras que en el segundo es una de las partes la que redacta las condiciones, quedando a la otra simplemente la posibilidad de aceptarlo en su totalidad o de rechazarlo. Con ánimo de reforzar esta descripción, y teniendo en cuenta que son el instrumento propio utilizado en la contratación por adhesión, sirva la definición que de las condiciones generales de la contratación nos da el artículo 1 de la Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación: "Son condiciones generales de la contratación las cláusulas predispuestas cuya incorporación al contrato sea impuesta por una de las partes, con independencia de la autoría material de las mismas, de su apariencia externa, de su extensión y de cualesquiera otras circunstancias, habiendo sido redactadas con la finalidad de ser incorporadas a una pluralidad de contratos". Cabe subrayar por tanto que desde el punto de vista jurídico, para hablar de contrato de adhesión, no basta únicamente con la imposición de las condiciones

---

[568] EUROCLOUD AUSTRIA. Cloud contracts. What providers and consumers should discuss. Version 1.0. 1 november 2012. Disponible en web: http://www.cloudingsmes.eu/wordpress/wp-content/uploads/2014/07/CLOUD_Contracts_EN1.pdf

[569] Esta posible dicotomía ha sido tenida en cuenta en el marco del RGPD donde se ha contemplado un mecanismo para hacer frente, en los aspectos correspondientes a la protección de datos con la finalidad de garantizar una particular protección a la pequeña y mediana empresa. Nos estamos refiriendo al elemento ya apuntado de la existencia de códigos de conducta. Esta cuestión será objeto de tratamiento en otra parte de este capítulo.
El elemento del tamaño como factor determinante de que nos encontremos ante un contrato de adhesión o un contrato negociado, en ROHRMANN, C.A. y CUNHA J.F.S.R. Some Legal Aspects of Cloud Computing Contracts. *Journal of International Commercial Law and Technology*. 2015. Vol.10 Nº.1. p. 37-45.
Desde una visión más genérica para distinguir el contrato de adhesión y el contrato de negociación, ver BALLUGUERA GÓMEZ, C. Diferencias entre el contrato por adhesión y el contrato por negociación. www.notariosyregistradores.org . Disponible en web: http://www.notariosyregistradores.com/CONSUMO/ARTICULOS/2014-diferencias-contratos-adhesion-negociacion.htm

por una de las partes, sino que será necesario que se incorporen a una pluralidad de contratos. En el caso del cloud, en la mayoría de las ocasiones, particularmente cuando el responsable sea una PYME y el proveedor una gran empresa[570], estaremos ante un contrato de adhesión, siendo posible la negociación en otros supuestos.



Fuente: elaboración propia

En aquellos supuestos en los que sí que cabe la negociación, siguiendo a Hon[571], se puede afirmar que los ámbitos sometidos a mayores exigencias por parte de los clientes son: la exclusión o limitación de responsabilidad, particularmente en lo que concierne a la integridad de los datos y a la recuperación en caso de desastre; los niveles de servicio, incluyendo la disponibilidad; la seguridad y la privacidad, particularmente en lo que concierne a los asuntos regulatorios bajo el paraguas de la Directiva europea; la cautividad y cláusulas de salida; la posibilidad de los proveedores de modificar las características del servicio unilateralmente; y los derechos de propiedad intelectual.

Lo cierto es que la realidad, y también la estadística[572], demuestran que en la mayoría de las ocasiones nos encontramos ante contratos de adhesión (*take it or leave it basis*) y además, por la propia naturaleza remota del servicio cloud, en muchas ocasiones se lleva a cabo en la modalidad *click-through* y *self-service*. Es cierto que la libertad contractual última radica

[570] Si bien nada impide la posibilidad de que se dé el esquema inverso. De hecho, los proveedores globales tienden a establecerlos de manera estandarizada y no negociable, los proveedores nacionales de gran tamaño también suelen facilitar este mismo tipo de contratos, pero sin embargo existe una mayor tendencia entre los proveedores más pequeños a facilitar soluciones a medida, donde el SLA es susceptible de negociación. TIME.LEX CVBA y SPARK LTD. Standards terms and performance criteria in service level agreements for cloud computing services. 2015. Disponible en web: http://www.sla-ready.eu/sites/default/files/Finalreport.pdf

[571] HON, K., MILLARD, C. y WALDEN, I. Negotiating Cloud Contracts: looking t clouds from both sides now. *Stanford Technology Law Review.* Ob. cit. p. 81.

[572] En una encuesta llevada a cabo por el *Cloud Industry Forum* en 2011, se observó que si bien el 45% de las organizaciones encuestadas utilizaban algún tipo de servicio cloud, solo el 52% (y en particular las grandes empresas) habían tenido alguna capacidad de negociación. Información extraída de HON, K., MILLARD, C. y WALDEN, I. ob. cit. p. 85.

en la posibilidad de no firmar el contrato, pero no es menos cierto, como afirma McGilliwray, que un consumidor (trasladable en este punto a las PYMES) probablemente encontrará condiciones similares, iguales para todos, de los proveedores competidores[573].

Un ejemplo claro de lo que estamos hablando, y siguiendo a Araiza[574], sería por un lado el contrato suscrito entre Google y la ciudad de Los Ángeles para el sistema de correo electrónico de los empleados y que incluía previsiones por las cuales Google compensaría a la ciudad en caso de que hubiera una vulneración del sistema y los datos de la ciudad quedaran expuestos o fueran robados; y por otro lado el servicio estándar de Gmail a disposición de cualquier usuario donde no cabe negociación alguna. Aunque no siempre esta ecuación de poder de las partes es válida, y basta ver por ejemplo cómo el prototipo Alpha.gov.uk, de una web única para todos los servicios online del gobierno británico, sostenido en el IaaS de Amazon, se contrató usando los términos y condiciones estándar[575].

Otra variable a tener en cuenta en la ecuación es que lógicamente el margen y la realidad de negociación es mucho mayor en el caso de las nubes privadas, también lógicamente a un mayor coste, que en el caso de las nubes públicas, donde la adhesión, se insiste, es la norma generalizada. La naturaleza pública de la nube es inversamente proporcional al precio y a la capacidad de negociación. A mayor customización de la nube, mayor precio y mayor capacidad de negociación. A ello matiza Hon que en los últimos años se está dando una tendencia en los proveedores nicho y en los integradores, que están más deseosos de acomodar sus servicios a los clientes, tanto en las condiciones contractuales como en las características del servicio; aunque reconoce que los grandes proveedores lo están haciendo ofreciendo diferentes modalidades de contratación en función de los sectores[576]; es decir, añadimos, estableciendo diferentes modelos de contratos de adhesión.

También desde la perspectiva de la naturaleza, y siguiendo a García del Poyo, podemos señalar un doble argumento a efectos de considerar estos contratos como mercantiles en aquellos casos, como estamos analizando, en que los mismos se lleven a cabo entre

[573] McGILLIVRAY, K. A right too far? Requiring cloud service providers to deliver adequate data security to consumers. *International Journal of Law and Information Technology*. 2016. nº 25. p. 1-25. Disponible en web: https://academic.oup.com/ijlit/article-lookup/doi/10.1093/ijlit/eaw011
[574] ARAIZA, A.G., Electronic Discovery in the Cloud. *Duke Law and Technology Review*. 2011. nº 10. p. 1-19. Disponible en web: http://dltr.law.duke.edu/2011/09/20/electronic-discovery-in-the-cloud/>
[575] HON, K., MILLARD, C. y WALDEN, I. Negotiating Cloud Contracts: looking t clouds from both sides now. Ob. Cit. p. 88 y 89.

[576] HON, K., MILLARD, C. y WALDEN, I. Negotiating Cloud Contracts: looking t clouds from both sides now. *Stanford Technology Law Review.* Ob. cit. p. 126-127.

empresas: el hecho de que el objeto del mismo lo constituye un acto de comercio de los regulados en el Código de Comercio, y el hecho de que la contratación se produce entre empresas en el ámbito de su negocio[577].

Por último, y en cuanto al tipo de contrato, la AEPD afirma que el cloud computing o computación en nube es una nueva forma de prestación de los servicios de tratamiento de la información, válida tanto para una empresa como para un particular y, también, para la Administración Pública[578]. Estamos por tanto ante un contrato de prestación de servicios, que cabe definir como aquel en el que una de las partes se obliga a prestar a la otra un servicio por un precio cierto (art. 1544 del Código Civil referido al arrendamiento de servicios)[579].

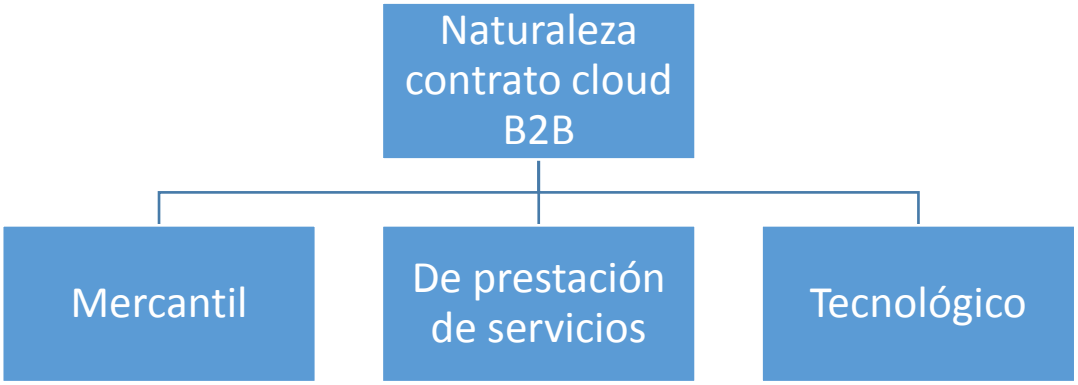
Hay quien subraya que existe el debate entre si nos encontramos ante un contrato de obras o de servicios[580]. Recordemos con la Sentencia de la Audiencia Provincial de Madrid de 14 de junio de 2005[581] que "El artículo 1544 del Código Civil se refiere a dos contratos distintos, por una parte, el arrendamiento de servicios, y, por otra parte, al de ejecución de obra. La diferencia entre ambos contratos radica en que, mientras en el arrendamiento de servicios, el arrendatario supedita su obligación de pagar el precio a la obligación del arrendador de prestaron servicio con independencia de la obtención o no de un resultado, en el de ejecución de obra el arrendatario supeditase obligación de pagar el precio a la obligación del arrendador de conseguir un resultado, sin que baste o sea suficiente la prestación por éste de un servicio adecuado y correcto si no se logra el resultado comprometido.

A nuestro juicio, reiteramos, estamos ante un contrato de servicios, de puesta a disposición de medios conforme a unas determinadas exigencias que refleja principalmente el Acuerdo de Nivel de Servicio al que ahora nos referiremos. No hay una exigencia de un resultado concreto, que es lo que implicaría un contrato de obra.

---

[577] GARCÍA DEL POYO, R. Cloud Computing: Aspectos jurídicos clave para la contratación de estos servicios. *reri.difusionjuridica.es*. p. 48-91. (p. 59.)
[578] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía para clientes que contraten servicios de Computing. Ob. Cit. p. 5.
[579] El Banco de España considera este tipo de contratos Cloud Computing, como una variedad del contrato de delegación de servicios o funciones, al que se refiere el apartado cuarto de la norma centésima quinta de la Circular 3/08, de 22 de Mayo, sobre determinación y control de los recursos propios mínimos. SALAS CLAVER, G. Algunos apuntes jurídicos sobre los contratos en Cloud Computing. Abril de 2013. Disponible en web: http://www.securitybydefault.com/2013/04/algunos-apuntes-juridicos-sobre-los_9.html
[580] Idem.
[581] España. Audiencia Provincial de Madrid. Sentencia de 14 de junio de 2005.

Otra nota definidora del contrato de cloud computing es que se trata de un contrato tecnológico. Siguiendo a Behar Quiñones y Yáñez Figueroa, podemos definir el contrato tecnológico como "un acuerdo de voluntad entre las partes que intervienen en una relación tecnológica, con los que se crean, transmiten, modifican o extinguen derechos y obligaciones relacionados con los sistemas informáticos o digitales"[582]. En el caso del cloud computing, por tanto, podemos concluir que estamos ante un contrato de este tipo por razón del objeto del servicio que se presta, que variará, tal y como hemos visto en el capítulo anterior, en función del modelo de servicio que se preste: SaaS, PaaS o IaaS. En palabras de Puyol Montero, el contrato de cloud es un contrato de prestación de servicios con flujo de datos informáticos[583]. En fin, la autoridad británica lo cataloga como un contrato de *outsourcing*[584].



Fuente: elaboración propia

3.4 Estructura y contenido del contrato.

No existe una regulación específica respecto a las características que deber reunir un contrato de este tipo, ya que estamos ante un contrato atípico, sino que han sido la práctica, las exigencias normativas generales (contratación civil y mercantil), y las vinculadas a aspectos concretos (laboral, propiedad intelectual…y fundamentalmente, en lo que nos afecta, la protección de datos…) las que los han ido delimitando. De hecho, solamente dos

[582] BEHAR QUIÑONES, G. y YAÑEZ FIGUEROA, A. *Introducción a los contratos tecnológicos*. Guadalajara, México, ITESO, 2014. 157 p.
[583] PUYOL MONTERO, J. *Algunas consideraciones sobre Cloud Computing*. Agencia Española de Protección de Datos. Agencia Estatal Boletín Oficial del Estado. Madrid. 2013. 273 p.
[584] INFORMATION COMMISSIONNER'S OFFICE (ICO). Guidance on the use of cloud computing. ob. cit. p. 4.

países de la UE, Eslovaquia y Luxemburgo, contienen sucintas referencias legislativas específicas a contratos de esta naturaleza[585].

Como hemos dejado ver al comienzo de este apartado, en el tratamiento doctrinal de esta cuestión, se ha focalizado el interés en la protección de datos, por ser, sin duda, un elemento crítico, pero hay que tener en cuenta que el contrato de prestación de servicios cloud es una fuente de obligaciones jurídicas que debe reunir una serie de requisitos propios de cualquier otro contrato: sujetos, objeto y causa; sin perjuicio de contemplar las especificidades derivadas de la nube y cumplir a su vez los exigentes requisitos derivados de la relación entre responsable y encargado.

Esta dicotomía se refleja en su estructura, ya que un contrato de prestación de servicios cloud habitualmente estará dividido en dos tipos de documentos[586]: un contrato marco propiamente dicho, y el conocido como Acuerdo de Nivel de Servicio, representado habitualmente a través de las siglas anglosajonas SLAs (*Service Level Agreements*)[587].

---

[585] En el caso de Eslovaquia su normativa sobre estándares de sistemas de información de la administración pública recoge definiciones de computación en nube, servicios de nube, acuerdos de nivel de servicio, usuario, proveedor, operador, intermediarios de servicios en nube y auditores de nube; y adicionalmente distingue y define IaaS, PaaS, y SaaS como modelos estándares de provisión de servicios en nube. En el caso de Luxemburgo hay previsiones específicas para la recuperación de los datos del usuario en el caso de una quiebra del proveedor. TIME.LEX CVBA y SPARK LTD. ob. cit. Disponible en web: https://ec.europa.eu/digital-single-market/en/news/study-report-standards-terms-and-performances-criteria-service-level-agreements-cloud-computing

[586] GARCÍA DEL POYO, R. Ob. cit. p. 63. También en la misma línea CLOUD SELECT INDUSTRY GROUP–SUBGROUP ON SERVICE LEVEL AGREEMENT (C-SIG-SLA). Cloud Service Level Agreement Standardisation Guidelines. 26 de junio de 2014. Disponible en web: https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines
Desde el punto de vista americano, se habla también de esta dicotomía, distinguiendo por un lado el acuerdo o contrato de suscripción (*Subscription Agreement*) y por otro el SLA. NOBLE FOSTER, T. Navigating Through the Fog of Cloud Computing Contracts. *J. Marshall J. Info. Tech. & Privacy*. 2013. Vol. 30. Issue 1. p. 13-30. Disponible en web: http://repository.jmls.edu/cgi/viewcontent.cgi?article=1727&context=jitpl

[587] No faltan quienes como Bernard Golden consideran que focalizarse en los SLA es inútil. GOLDEN, B. The Death of the SLA. *CIO FROM IDG.* 17 de febrero de 2015. Disponible en web: http://www.cio.com/article/2883770/cloud-computing/the-death-of-the-sla.html No obstante, cabe subrayar que incluso hay quienes sostienen que la ausencia del SLA podría ser causa de nulidad del contrato al no ser determinable la obligación. Así lo señala el experto rumano del estudio de TIME.LEX CVBA y SPARK LTD. ob. cit. p.7.
Existen además otras clasificaciones como la ofrecida por Stefan Frey, Claudia Luthje y Christoph Reich, del *Cloud Research Lab* de la Universidad de Furtwagen (Alemania) que consideran que todo es susceptible de ser incluido en el SLA, distinguiendo cuatro partes: elementos referidos al acuerdo, elementos referidos al servicio, elementos referidos a la documentación y elementos referidos a la gestión. FREY, S., LUTHJE, C., y REICH, C. Key Performance Indicators for Cloud Computing SLAs. *IARIA.* 2013. p. 60-64. De similar modo, la ENISA señala que "en los SLAs están resueltas, o al menos mitigadas, las consideraciones de numerosas cuestiones legales asociadas con la computación en nube". ENISA. Computación en nube. Beneficios, riesgos y recomendaciones para la seguridad de la información. Ob. cit. p. 109.
Los SLA han sido tradicionalmente utilizados por las operadoras de telecomunicaciones. EUROPEAN TELECOMMUNICATIONS STANDARD INSTITUTE. Cloud; SLAs for Cloud Services. Technical Report. p.

3.4.1 El contrato marco.

El contrato marco deberá recoger en primer lugar la identificación de las partes, cuestión profusamente tratada más arriba en el plano de la protección de datos y que no presenta particularidades en otra perspectiva: el prestador de servicios en nube y el cliente, actuando en el plano de la privacidad el primero como encargado del tratamiento y el segundo como responsable, respecto a los datos de terceros. También será necesario que se fije el objeto del contrato, que en línea con la definición dada, será la prestación de un servicio a cambio de una remuneración.

En cuanto a las obligaciones de las partes, las vamos a ir viendo en las próximas líneas, por cuanto se ven plasmadas en cláusulas que van tratando diversas cuestiones: la modalidad del servicio de computación en nube que se presta, la contraprestación a satisfacer por el cliente/responsable de los datos y la facturación, los aspectos concernientes a la propiedad intelectual [588], entrada en vigor, duración del contrato y su prórroga, pactos de confidencialidad, portabilidad y cláusulas de salida, fuero o jurisdicción y normativa aplicable (con todas las limitaciones derivadas de la normativa de protección de datos a las que se ha hecho mención en los apartados anteriores). En fin, en el análisis comparativo llevado a cabo por Colom Planas de diferentes propuestas de clausulado contractual[589] se pueden señalar otras no mencionadas entre las que estarían algunas de las cuestiones que se van a tratar con gran detalle en otros apartados de este capítulo y en el próximo capítulo, por encontrarse directamente vinculadas con la privacidad: la seguridad de los datos, las transferencias internacionales de datos en su caso, los mecanismos de auditoría, la subcontratación o las

6. Disponible en web: https://www.etsi.org/deliver/etsi_tr/103100_103199/103125/01.01.01_60/tr_103125v010101p.pdf

[588] La ENISA recuerda al respecto que "en el caso de IaaS y PaaS, puede almacenarse la propiedad intelectual, incluidas las obras originales creadas utilizando la infraestructura de nube. El cliente en nube debe asegurarse de que el contrato respeta sus derechos sobre cualquier propiedad intelectual o trabajo original en la medida de lo posible, sin comprometer la calidad del servicio ofrecido (por ejemplo, las copias de seguridad podrían ser un elemento necesario a incluir en una oferta de nivel de servicio satisfactorio). ENISA. Computación en nube. Beneficios, riesgos y recomendaciones para la seguridad de la información. 2009. p. 95. Para ver la importancia de esta materia desde la perspectiva de otro ordenamiento, TEMPERINI, M.G.I. Propiedad Intelectual: La cesión de licencias como elemento esencial en los Servicios Cloud Computing. *Jornadas Argentinas de Informática Nº 40 (JAIIO 40) - Simposio de Informática y Derecho*. 2011. Disponible en web: http://www.elderechoinformatico.com/publicaciones/mtemperini/JAIIO_CC_PI_Temperini.pdf

[589] COLOM PLANAS, J.L. Cláusulas contractuales en entornos de *cloud computing*. 5 de octubre de 2012. Disponible en web: http://www.aspectosprofesionales.info/2012/10/clausulas-contractuales-en-entornos-de.html que plantea un contenido de diferentes cláusulas en función de las aportaciones llevadas a cabo por distintos autores, entidades y organizaciones, y en concreto las siguientes: CSA (Cloud Security Alliance), ENISA (European Network and Information Security Agency), Thomas Trappler en su libro "*Contracting for cloud services"*, Xabier Ribas, el INTECO (hoy INCIBE) y el capítulo italiano de la Cloud Security Alliance.

respuestas ante incidencias en el servicio. También en ocasiones, sea dentro de la cláusula de distribución de responsabilidades o sea en una cláusula diferente, se recogen las advertencias respecto al acceso por parte de las autoridades públicas, cuestión esta que reiteramos la trataremos con detalle posteriormente.

3.4.2 El Acuerdo de Nivel de Servicio (SLA)

Habitualmente, como un anexo (y en ocasiones como contenido incorporado al contrato mismo), nos encontramos con el SLA o Acuerdo de Nivel de Servicio, en el que básicamente se reflejan los aspectos técnicos del servicio prestado[590]: la lista de servicios que el proveedor facilitará y una completa definición de cada servicio, las métricas para determinar si un proveedor está prestando el servicio como prometió y un mecanismo de auditoría para monitorizar el servicio, las responsabilidades del proveedor y del cliente y las soluciones disponibles para ambos si no se cumplen los términos del SLA, así como una descripción de cómo cambiará el SLA con el tiempo. De una manera simplificada, Wagle lo define como un documento formal que define (o intenta definir) en términos cuantitativos y cualitativos, el servicio ofrecido a los usuarios[591]. En términos complementarios, no faltan quienes sostienen que una buena práctica es precisamente detallar aquellos tipos de servicios que no están incluidos en el SLA[592].

Entrando ya en un mayor detalle, uno de los contenidos más relevantes de un SLA es el denominado a su vez SLO u Objetivo de Nivel de Servicio, que define las condiciones objetivamente establecidas para medir el servicio prestado. Los indicadores pueden ser de rendimiento, velocidad de procesamiento, ancho de banda, latencia en los sistemas, entre otros. Uno de los más relevantes a su vez es el de los porcentajes de disponibilidad para máquinas virtuales y otros recursos e instancias. En todo caso, resulta relevante la capacidad de medición de los mismos. Como señala el NIST “para tener éxito en la provisión de servicios en nube, uno tiene que tener requisitos claros, crear acuerdos de nivel de servicios

---

[590] IBM. Review and summary of cloud service level agreements - From Cloud Computing Use Cases Whitepaper Versión 4.0. Disponible en web: http://public.dhe.ibm.com/software/dw/cloud/library/cl-rev2sla-pdf.pdf

[591] WAGLE, S.S., Cloud Computing Contracts: Regulatory Issues and Cloud Providers’ Offer: An nalysis. *Research Work. University of Luxembourg.* Disponible en web: http://www.ifip-summerschool.org/wp-content/uploads/2016/08/IFIP-SC-2016_pre_paper_11.pdf

[592] EXPERT GROUP MEETING ON CLOUD COMPUTING CONTRACTS. Synthesis of the meeting of 29/30 January 2014. Disponible en web: http://ec.europa.eu/justice/contract/files/expert_groups/29_30_jan_meeting_final_synthesis_en.pdf

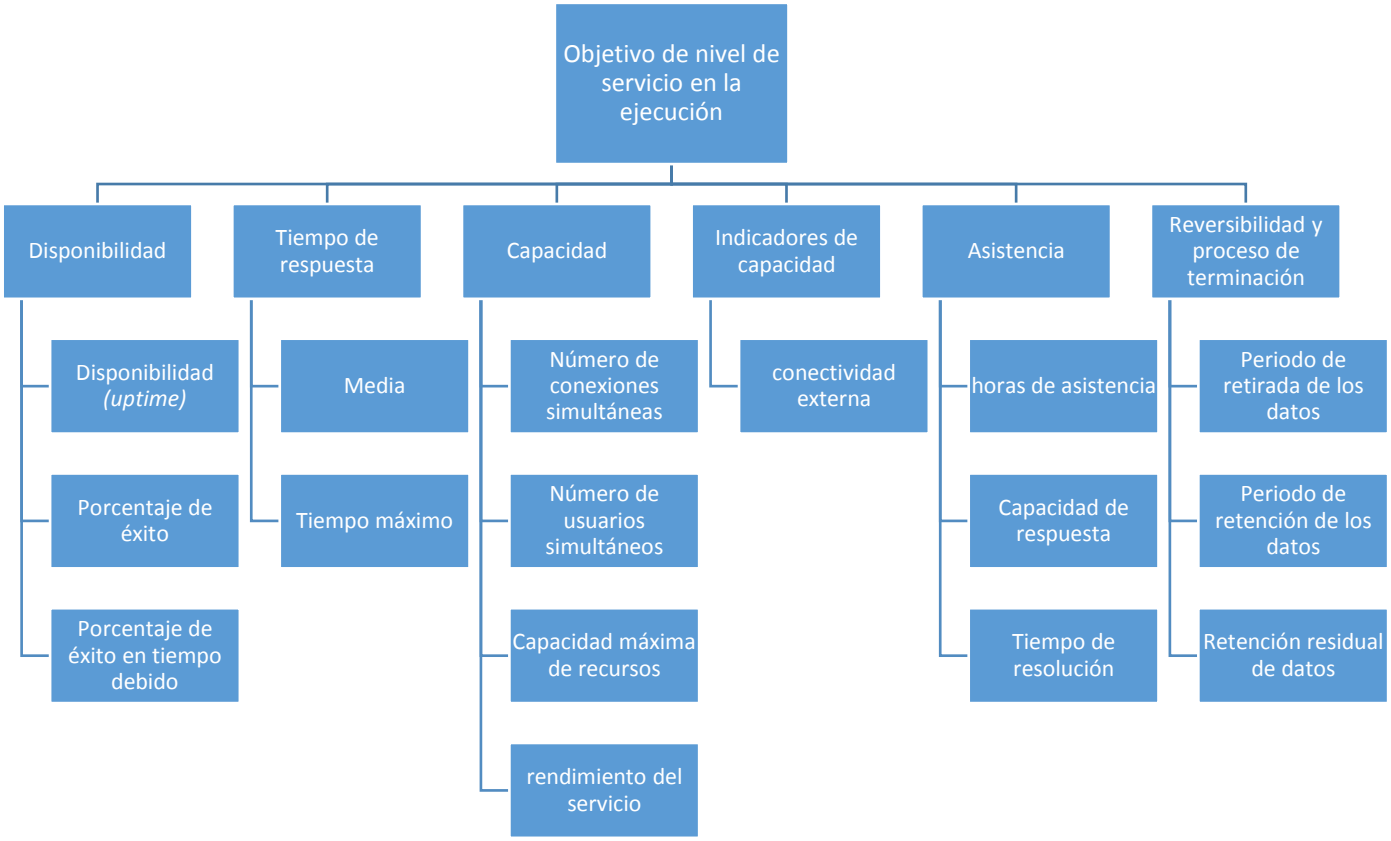
que reflejen esos requisitos y que sean medibles de cara a validar la prestación de esos servicios junto con su ejecución y recursos"[593].

Siguiendo al Subgrupo sobre Acuerdo de Nivel de Servicio del *Cloud Select Industry Group* (conocido por sus siglas C-SIG-SLA)[594], se pueden señalar dentro del apartado concerniente al **objetivo del nivel de servicio en su ejecución**, los siguientes parámetros a incluir,

[593] NIST CLOUD COMPUTING REFERENCE ARCHITECTURE AND TAXONOMY WORKING GROUP. Cloud Computing Service Metrics Description. Disponible en web: http://www.nist.gov/itl/cloud/upload/RATAX-CloudServiceMetricsDescription-DRAFT-20141111.pdf
En la misma línea, ZALAZAR, A.S., GONNET, S. y LEONE, H. Aspectos Contractuales de Cloud Computing. *Tercer Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática (CIIDDI)*. Mar del Plata, Argentina. 2014. Disponible en web: http://www.ciiddi.org/congreso2014/images/documentos/aspectos%20contractuales%20de%20cloud%20computing%20zalazar.pdf
"Los indicadores utilizan métricas, que se asocia a una determina medida, y esta tiene una unidad y una función de cálculo. Los valores actuales de las métricas se van generando de acuerdo al método de colección (por nanosegundo, minuto, horas, etc.) que estas posean. El monitor de servicio deberá auditar los valores e indicar cuándo se encuentren fuera del nivel objetivo de servicio, que es donde se indicará una penalidad a ejecutar".

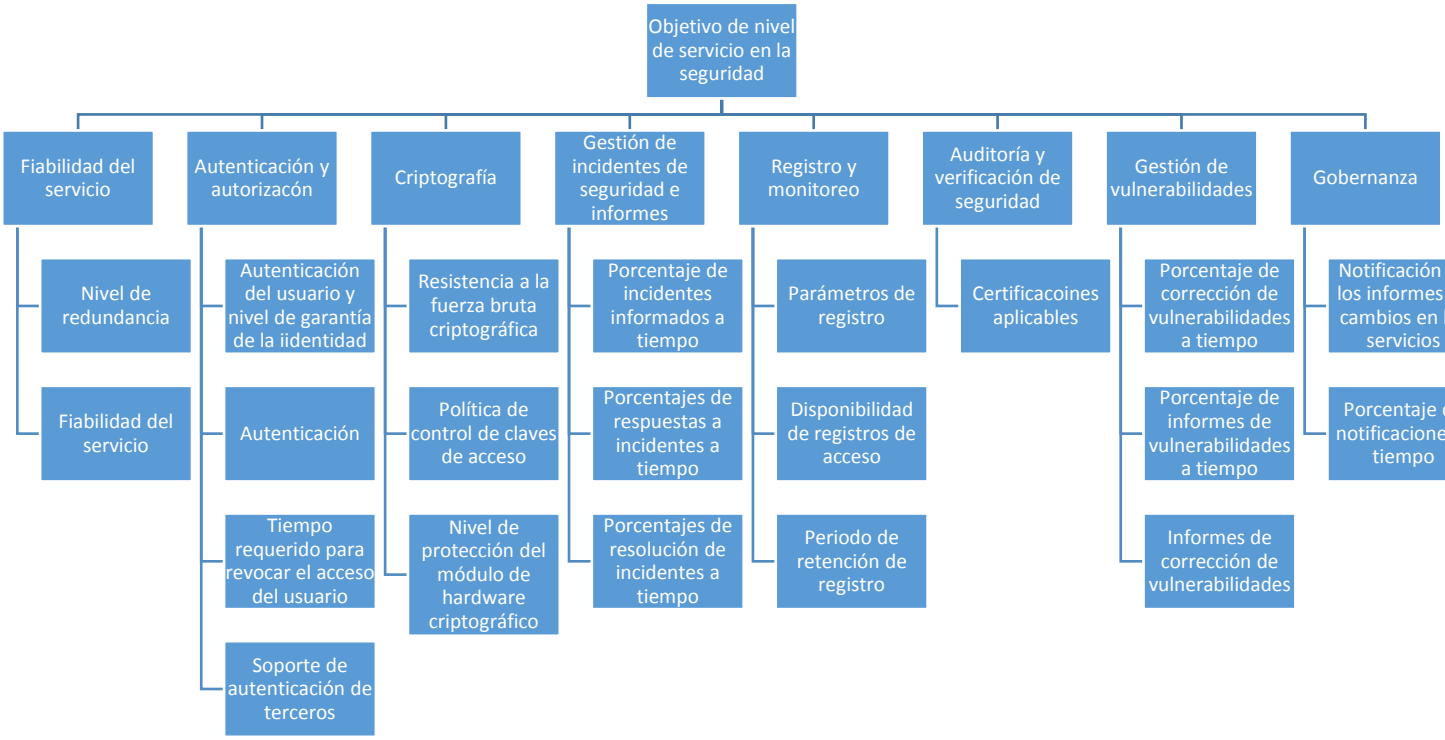
[594] CLOUD SELECT INDUSTRY GROUP–SUBGROUP ON SERVICE LEVEL AGREEMENT (C-SIG-SLA). Cloud Service Level Agreement Standardisation Guidelines. Ob. cit. p. 15 y siguientes. La labor de este Grupo de trabajo, que tiene el respaldo de la Comisión Europea, responde a que los SLA son un componente importante de la relación contractual entre el cliente y el proveedor de un servicio cloud. Debido a la naturaleza global de la nube, los SLA habitualmente abarcan distintas jurisdicciones, con requisitos legales habitualmente diferentes, en particular en lo que concierne a la protección de los datos personales almacenados por el servicio en nube. A mayor abundamiento los diferentes servicios *cloud* y modelos de implantación requerirán diferentes enfoques de los SLA, añadiéndoles complejidad. Finalmente, la terminología de los SLA habitualmente difieren de un proveedor a otro, haciendo difícil que los clientes puedan comparar los servicios. A nuestro juicio todas estas dificultades hacen que la contribución de un grupo de este tipo en el que están presentes la mayoría de los grandes proveedores de este tipo de servicios y el respaldo de las autoridades europeas, suponen una manifestación concreta de colaboración público-privada en el plano normativo, que favorece el cumplimiento normativo derivado de las distintas exigencias legales, fijando los elementos comunes o estándares que pueden cumplir con las exigencias normativas diversas a través de un instrumento único. Es un ejemplo de autorregulación digno de mención.
Existen otros trabajos similares como por ejemplo el derivado del Grupo de Expertos sobre contratos de cloud computing establecido por la Comisión Europea a través de su Decisión de 18 de junio de 2013. EUROPEAN_COMMISSION. DECISION of 18 June 2013 on setting up the Commission expert group on cloud computing contracts. Disponible en web: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:174:0006:0008:EN:PDF
Este grupo de expertos se estableció para asesorar a la Comisión en la identificación de términos y condiciones seguros y adecuados para los servicios de cloud computing dirigidos a consumidores y pequeñas empresas. Realizó diversos trabajos y seminarios durante el año 2014 (información disponible en web: http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm) pero sin embargo los trabajos se pararon y no concluyeron. Algunas de las afirmaciones se recogerán a lo largo de este trabajo, sin que se les pueda dar ninguna naturaleza oficial.
De manera mucho más reciente encontramos el elaborado por el SLALOM Project, confinanciado por la Unión Europea, enfocado al ámbito del cloud específicamente e impulsado por las siguientes entidades: consultores del proveedor de servicios mundial Atos, de la firma jurídica Bird and Bird, investigadores de la Universidad Técnica nacional de Atenas y de la Universidad del Pireo, y el Cloud Industry Forum. SLALOM. Model Contract for Cloud Computing. 21 de marzo de 2016. Disponible en web: http://slalom-project.eu/sites/slalom/files/content-files/article/SLALOM%20Legal%20model_clauses%20only_v1.2.pdf

aunque cabra la posibilidad de que en determinadas ocasiones y en función de la modalidad de servicio prestado, algunos de los mismos no estén: disponibilidad, entendiendo como tal la propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada; el tiempo de respuesta, es decir el intervalo de tiempo entre la petición llevada a cabo por el cliente y la respuesta del proveedor a dicha solicitud; capacidad, entendida como la cantidad máxima de alguna propiedad del servicio en nube (por ejemplo el número de accesos simultáneos o el número de conexiones simultáneas…); indicadores de la capacidad, que son objetivos de nivel de servicio que prometen funcionalidades específicas relativas al servicio; asistencia, es decir la interfaz puesta a disposición por el proveedor para gestionar las cuestiones planteadas por el cliente; y la reversibilidad y proceso de terminación, que hace referencia a los pasos que permiten al cliente recuperar sus datos en un determinado periodo de tiempo antes de que el proveedor proceda a su eliminación del sistema.



Fuente: elaboración propia con base en los criterios de C-SIG-SLA

A ello añaden otra serie de contenidos vinculados a la seguridad, es decir a los **objetivos del nivel de servicio en seguridad**. En este caso, se incluirán: la fiabilidad del servicio, es decir la propiedad del servicio para realizar su función correctamente y sin fallos, particularmente en un determinado periodo de tiempo (particular relevancia tienen aquí las certificaciones); autenticación y autorización, siendo el primero la verificación de una identidad declarada por una entidad (el cliente), y el segundo un proceso de verificación de que una entidad tiene permiso para acceder y utilizar un particular recurso basado en unos privilegios del usuario predefinidos; criptografía, que es una técnica que permite la transformación de los datos de cara a esconder la información contenida, prevenir su modificación no detectada y/o prevenir su uso no autorizado (encriptación); gestión de los incidentes de seguridad e informe, entendido como los procesos para detectar, informar, afrontar, responder y lidiar con los incidentes de seguridad; auditoría y verificación de seguridad, que es el proceso sistemático, independiente y documentado para obtener una evidencia auditada sobre un servicio *cloud y* evaluarlo objetivamente para determinar en qué medida los criterios de auditoría se cumplen; gestión de vulnerabilidades, que significa que la información sobre las vulnerabilidades técnicas de los sistemas de información utilizados deberá obtenerse de manera oportuna, la exposición de la organización a dichas vulnerabilidades evaluadas y las medidas apropiadas adoptadas para hacer frente a ese riesgo asociado; gobernanza, el sistema por el cual el servicio es dirigido y controlado, con particular referencia a la forma en la que los cambios y actualizaciones del servicio son gestionados, en función de si el cambio viene originado por el cliente o por el proveedor.



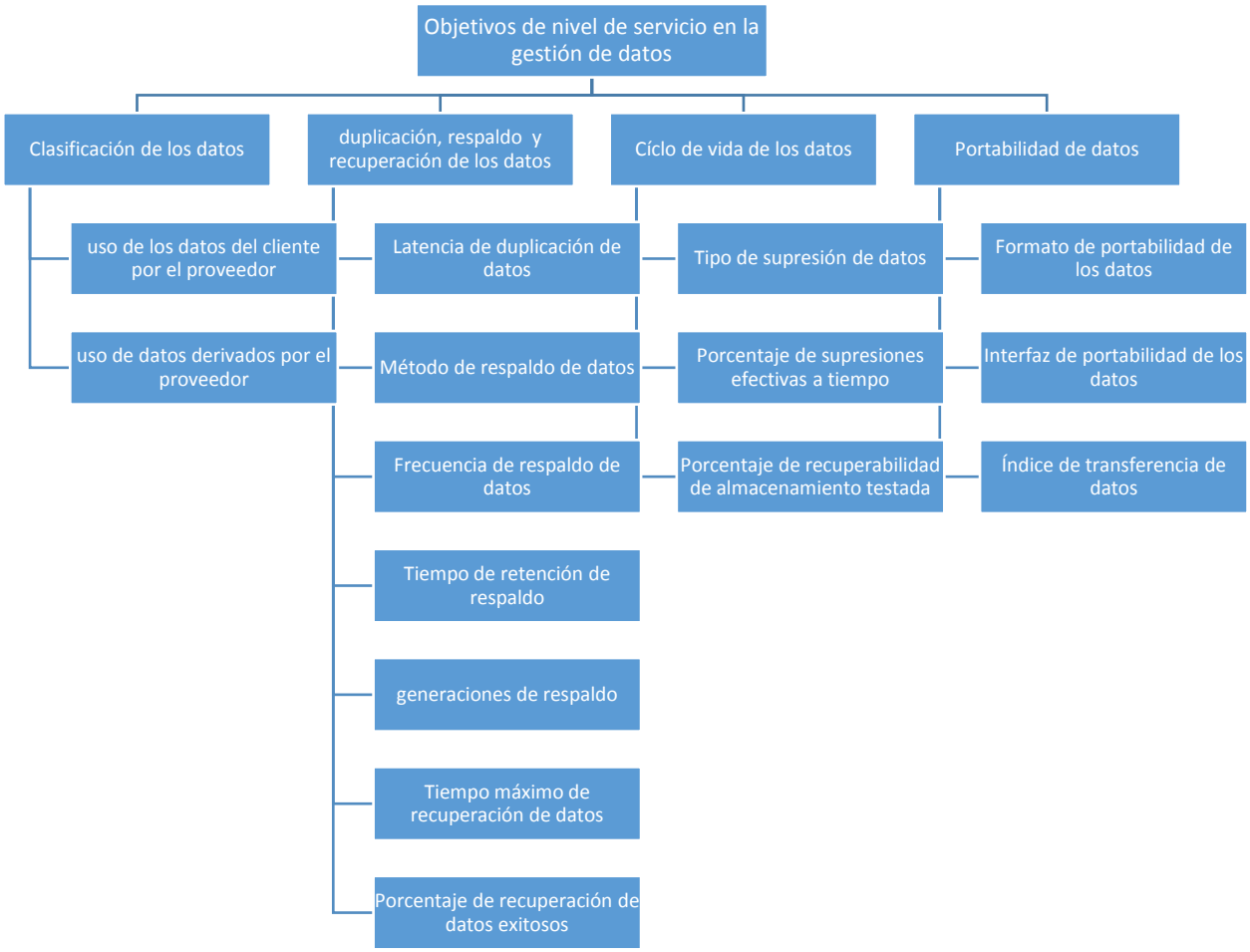
Fuente: elaboración propia con base en los criterios de C-SIG-SLA

También en el plano de los objetivos del nivel de servicio, y siguiendo con los parámetros fijados por el C-SIG-SLA, están incluidos específicamente los referidos a los datos, tanto en su vertiente de **gestión de los datos**, como en lo referido específicamente a la **protección de datos personales**. Antes de entrar en el contenido cabe citar que existen quienes distinguen entre el SLA (que servirían para proveer métricas y otro tipo de información acerca del rendimiento de los servicios) y el PLA (*Privacy Level Agreement)* que sirve para describir el nivel de protección de la privacidad que el proveedor de servicios cloud ofrece[595].

En referencia a lo primero, la gestión, se sitúa la clasificación de los datos, es decir, la descripción de los tipos de datos que están asociados al servicio en nube (datos del cliente, del proveedor y datos derivados), así como el uso de los datos del cliente y de los datos derivados; la duplicación (*mirroring)*, respaldo (*backup*) y recuperación (*restore*) de los datos,

[595] CLOUD SECURITY ALLIANCE. GRUPO DE TRABAJO-PRIVACY LEVEL AGREEMENT. Esquema de Privacy Level Agreement (PLA) para la Venta de Servicios en la Nube en la Unión Europea, julio de 2013. Disponible en web:https://www.ismsforum.es/ficheros/descargas/acuerdo-de-nivel-de-privacidad1374159133.pdf

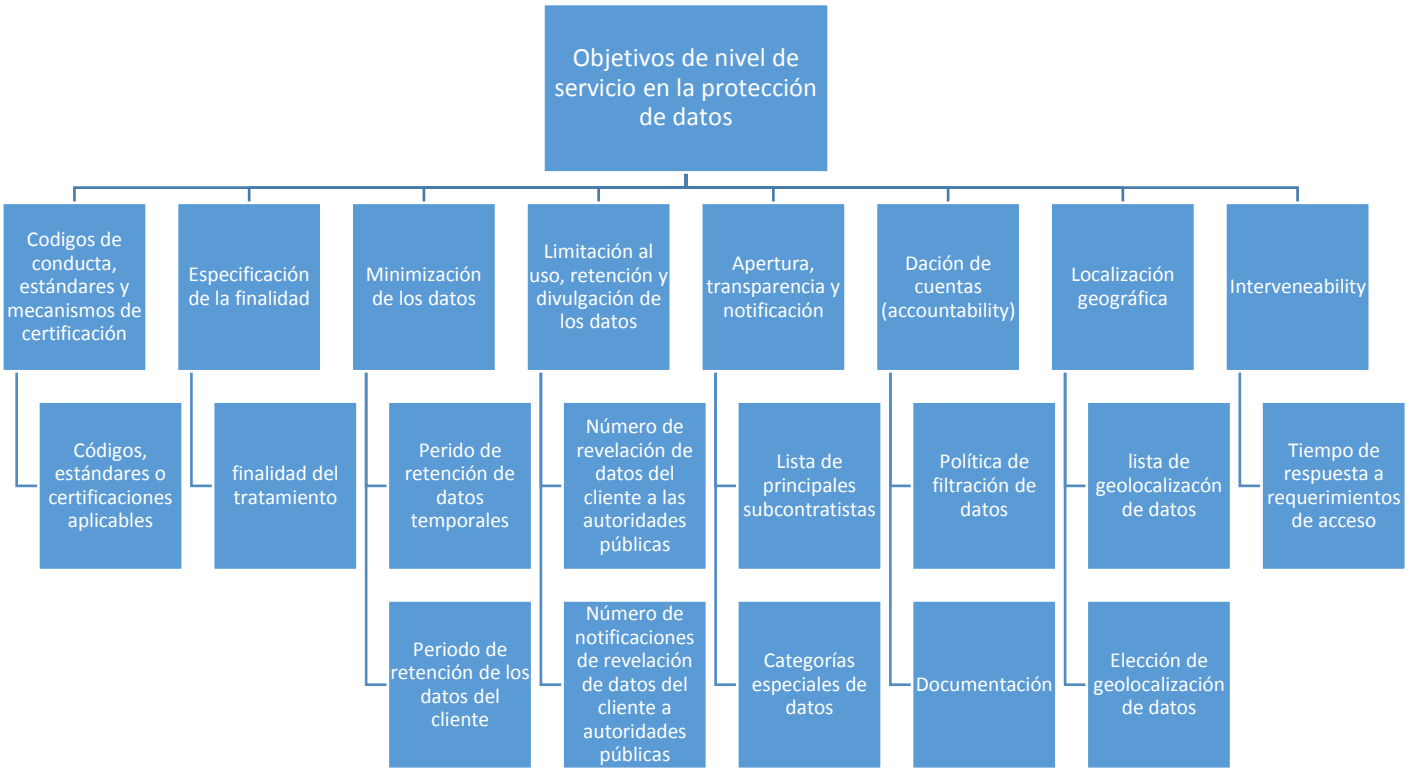
es decir, los mecanismos utilizados para garantizar que los datos de los clientes están disponibles en caso de fallos que impidan el acceso a los mismos; el ciclo de vida de los datos, es decir, la eficiencia y efectividad de las prácticas de ciclo de vida de los datos del proveedor, con una particular atención en las prácticas y mecanismos para el tratamiento y el borrado de los datos; y la portabilidad de los datos, es decir, lo referido a las capacidades del proveedor para exportar datos de tal modo que puedan seguir siendo utilizados por el cliente en caso de que termine la relación contractual.



Fuente: elaboración propia con base en los criterios de C-SIG-SLA

En lo que concierne a la **protección de datos personales en sentido estricto** se incluirán los aspectos que, como vamos a desarrollar en los próximos apartados, nos exige en gran medida la normativa de protección de datos**:** los mecanismos de certificación, estándares o

códigos de conducta de que disponga o a los que esté adherido el proveedor; especificación de la finalidad del tratamiento, de tal modo que no puedan ser objeto de tratamiento por el proveedor para una finalidad distinta; minimización de los datos, de tal modo que se incluyan previsiones claras respecto a la supresión de los datos; limitación respecto al uso, retención y divulgación de los datos, debiendo informar al cliente, a la mayor brevedad posible en función de las circunstancias, de cualquier requerimiento o mandato legal en virtud del cual el proveedor esté obligado a desvelar datos personales por un mandato legal o una autoridad gubernamental, salvo que esté prohibido por ejemplo para preservar la confidencialidad de una investigación; apertura, transparencia y notificación, de tal modo que el proveedor deberá facilitar toda la información que permita al cliente proveer al interesado con una notificación adecuada sobre el tratamiento de sus datos personales, como exige la ley; responsabilidad, que describe la capacidad de las partes para demostrar que adoptaron todas las medidas necesarias para asegurar que los principios de protección de datos han sido implantados. Esta última es particularmente importante de cara a investigar las vulneraciones de datos personales, para lo que el proveedor deberá facilitar mecanismos de identificación y monitoreo fiables; localización geográfica de los datos almacenados; y cláusulas respecto al cumplimiento de los derechos ARCO, de tal modo que se refleje que el proveedor está obligado a apoyar al cliente a la hora de facilitar el ejercicio de los referidos derechos a los interesados de una manera eficiente y puntual.



Fuente: elaboración propia con base en los criterios de C-SIG-SLA

La cláusula de protección de datos es de las más relevantes y la que ahora nos va a ocupar. Resulta en este sentido importante distinguir, en línea con lo que ya se ha apuntado, que concurrirá en realidad una cláusula con un contenido doble: por un lado estará la recogida de los datos del cliente en sí mismo, es decir actuando el proveedor como responsable, y por otro estará la posibilidad de acceder a los datos de terceros tratados por el cliente pero que van a ser a su vez tratados por el proveedor en su condición de encargado. Esta última relación viene informada por un contenido obligatorio que se deriva en gran medida de los artículos a los que antes hemos hecho mención y que marcan particularmente las obligaciones que asumen las partes. Así, el artículo 17 de la Directiva 95/46 dice que será necesario que el clausulado incluya que el encargado solo actúa siguiendo instrucciones del responsable y que las obligaciones referidas a las medidas de seguridad incumben directamente al encargado. De similar manera se pronuncia el artículo 12 LOPD que señala que se deberá recoger expresamente que el encargado 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; a lo que se añadirá el contenido concerniente a las medidas de seguridad.

Elemento clave por tanto son las instrucciones, en cuanto que reflejo del control del tratamiento de los datos, que constituyen el elemento determinante de la relación entre responsable y encargado. En el ámbito de la nube, la generalizada presencia de los contratos de adhesión hace que la definición de los servicios a prestar venga fijada por el propio proveedor y es el cliente el que acepta o no. Compartimos en este sentido la opinión de Rubí Navarrete de que desde el punto de vista normativo, con esa posibilidad, esa aceptación o no, esa libertad contractual última a la que ya nos hemos referido, así como la determinación de los servicios concretos que contrata (recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción)[596] se puede entender que el cliente está instruyendo al proveedor sobre los términos en los que deberá proceder en cuanto al tratamiento de los datos personales[597]. Se equipararía por tanto instrucción a servicios.

Además no cabe que el proveedor utilice los datos con una finalidad distinta de la del tratamiento que le ha sido encomendado, para lo cual será necesario atender muy estrechamente a los términos y condiciones de uso que establece el correspondiente contrato. Además, el último inciso del precepto transcrito señala otros dos elementos fundamentales: la imposibilidad de que el proveedor comunique los datos a otras personas y el contenido concerniente a las medidas de seguridad. Estos dos últimos elementos, la subcontratación y las medidas de seguridad –de gran importancia por su carácter consustancial a la naturaleza del cloud en el primero de los casos, y elemento de preocupación generalizada en el segundo– serán tratados con detalle en otros apartados de esta obra, por lo que no nos extendemos más en este momento, más allá de algún apunte mínimo necesario. En línea con lo transcrito, el art. 20 ROPD recoge que en caso de que se incumplan las instrucciones o que el proveedor destine los datos a una finalidad distinta de la indicada por el cliente, entonces surgirá el elemento de la corresponsabilidad.

[596] Enumeración recogida en AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Directrices para contratos responsable – encargado. 2017. Disponible en web: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/directricescontratos.pdf

[597] RUBÍ NAVARRETE, J. El proveedor de cloud como encargado del tratamiento, en MARTÍNEZ MARTÍNEZ, R (Ed.). *Derecho y Cloud Computing.* Thomson Reuters. 2012. p. 87 a 107.

El RGPD ha sido más exigente –o al menos más detallista– en línea con lo que venía opinando el Grupo de Trabajo del artículo 29[598], y algo lógico si se compara la naturaleza del instrumento jurídico del reglamento comunitario como fuente frente a la directiva. En concreto el artículo 26 señala que el contrato establecerá la materia y duración del tratamiento, la naturaleza y finalidad del tratamiento, el tipo de datos personales y las categorías de interesados, los derechos y obligaciones del responsable, e incluirá en particular una serie de disposiciones.[599] Algunas replican las anteriormente mencionadas. Así, se recoge el tratamiento de los datos solamente siguiendo las instrucciones del responsable, salvo que así se lo exija el Derecho de la Unión o de un Estado Miembro al que esté sometido el encargado; en cuyo caso deberá informar al responsable del requerimiento legal antes de tratar los datos, salvo que la norma prohíba facilitar dicha información en asuntos de importante interés público; y sin perjuicio, como recuerda la AGPD, de que el encargado/proveedor, pueda adoptar todas las decisiones organizativas y operacionales necesarias para la prestación del servicio que tenga contratado[600]. En este campo de las instrucciones, se recoge igualmente un deber de vigilancia normativa, o de *compliance* en la labor del proveedor, que en cuanto que encargado, cuando aprecie una instrucción del responsable contraria a la normativa, deberá comunicarlo al cliente.

También, en línea con lo antes reflejado, deberá tomar las medidas de seguridad que exige el RGPD en su art. 30 en lo concerniente al tratamiento de los datos, asegurarse de que las personas autorizadas para tratar los datos se han comprometido a respetar la confidencialidad y respetar las condiciones de la norma en caso de contratar otro encargado, algo que, como hemos apuntado más arriba, es extraordinariamente frecuente en el caso de la computación en nube.

También en el plano de la seguridad, se recogerá la ayuda al responsable garantizar el cumplimiento de las obligaciones en materia de seguridad de los datos considerando la

[598] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 05/2012 sobre la computación en nube. 1 de julio de 2012. Disponible en web: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_es.pdf

[599] Este nivel de detalle ha sido aplaudido por las autoridades de control quienes han señalado que "el Grupo de Trabajo se congratula de las disposiciones contenidas en el artículo 26 de la propuesta de la Comisión (proyecto de Reglamento general de protección de datos de la UE) que tiene como objetivo hacer que los encargados del tratamiento respondan en mayor medida frente a los responsables del tratamiento, ayudándoles a garantizar el cumplimiento de la normativa, en particular en materia de seguridad y obligaciones conexas". GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 05/2012 sobre la computación en nube. ob. cit. p. 26.

[600] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Directrices para contratos responsable – encargado. 2017. Ob. cit. p. 3.

naturaleza del tratamiento y de la información a disposición del encargado; así como la puesta a disposición del responsable de toda la información necesaria para demostrar el cumplimiento de las obligaciones (la notificación de violaciones de datos a las autoridades de control, la comunicación de violaciones de datos a los interesados, la realización de las evaluaciones de impacto relativa la protección de datos y, en su caso, la realización de consultas previas)[601] y permitir y contribuir a las auditorías, incluyendo las inspecciones dirigidas por el responsable u otro auditor mandatado por el responsable. Esto último, en línea con lo previsto por el art. 20.2 del ROPD y en el art. 88.5 y 6 ROPD, se proyectará también en el documento de seguridad[602]. Precisamente lo referido a la auditoría puede plantear problemas en el caso del cloud computing ya que es frecuente que no sea el cliente el que elija al auditor y mucho menos que audite personalmente, sino que será frecuente la auditoría por un tercero independiente designado por el proveedor[603]. En todo caso, sobre esta cuestión nos detendremos en el apartado referido a las medidas de seguridad, igual que haremos al tratar las cláusulas de salida respecto de la obligación del proveedor, a elección del cliente, de borrar o devolver los datos al responsable después de la terminación de los servicios de tratamiento de los datos y borrar las copias existentes, salvo que el Derecho de la Unión o del Estado Miembro requiera del almacenamiento de los datos, disposición esta que hoy día ya recoge en gran medida el art. 22 ROPD.

Dentro del contenido, se añaden también cláusulas específicas de colaboración entre el responsable y el encargado, el proveedor y el cliente. Es el caso de la asistencia al cliente mediante medidas técnicas y organizativas para el cumplimiento de las obligaciones del responsable para hacer frente a los requerimientos para el ejercicio de los derechos por los interesados. De nuevo la AEPD afirma que "el proveedor de cloud debe garantizar su cooperación y las herramientas adecuadas para facilitar la atención de dichos derechos"[604]. Al respecto señala que el acuerdo deberá establecer de forma clara si corresponde al

---

[601] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Directrices para contratos responsable – encargado. 2017. Ob. cit. p. 9.

[602] Para un mayor detalle ver AGENCIA ESPAÑLA DE PROTECCIÓN DE DATOS. Informe 0457/2008. Disponible en web: https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/medidas_seguridad/common/pdfs/2008-0457_Obligaci-oo-n-del-responsable-del-tratamiento-de-datos-de-velar-que-el-encargado-cumpla-las-medidas-de-seguridad.pdf

[603] Ver al respecto. AGENCIA ESPAÑLA DE PROTECCIÓN DE DATOS. Informe 0464/2012. Disponible en web: https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2012-0464_Contrataci-oo-n-de-servicio-de-cloud-computing-por-cl-ii-nica-m-ee-dica.pdf

[604] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía para clientes que contraten servicios de Computing. ob. cit. p. 18.

encargado del tratamiento atender y dar respuesta a las solicitudes de estos derechos. En todo caso, lo veremos en el apartado correspondiente.

A continuación en la tabla se expone la comparativa del grado de detalle que informa la relación contractual entre el proveedor y el cliente.

CONTENIDO DEL CONTRATO			
Directiva	LOPD	ROPD	RGPD
el prestador sólo actúa siguiendo instrucciones del cliente	el prestador únicamente tratará los datos conforme a las instrucciones del cliente	Servicios objeto de subcontratación y en su caso empresa que los presta	Tratar los datos solamente siguiendo las instrucciones del responsable y acceso por autoridades públicas
las obligaciones de seguridad incumben también al prestador.	las medidas de seguridad que el prestador ha de implantar		tomar todas las medidas que concernientes a la seguridad
			Respetar las condiciones del RGPD en caso de subcontratar
			Compromiso de confidencialidad de las personas del proveedor que tengan acceso
			Asistencia al cliente en la satisfacción de los derechos de los interesados
			Borrado o devolución de datos

			Puesta a disposición de información del cliente y permiso para auditorías

Fuente: elaboración propia

Aquí se plantea una duda a desarrollar en la práctica una vez entre en vigor el RGPD. ¿Bastará con una remisión genérica al cumplimiento de la normativa o será necesario descender al detalle? El hecho de que el RGPD haya incorporado un mayor grado de detalle puede resultar indiciario de la necesidad de que los contratos de prestación de este tipo de servicios incluyan todo este contenido, aunque también en aras de la economía contractual, cabría interpretar que bastaría con una remisión a la normativa.

El modelo de clausulado que han elaborado las agencias de control española, catalana y vasca lleva a pensar que la primera opción es por la que se están inclinando. A ello parece inclinarse también la jurisprudencia. Como ha señalado el Tribunal Supremo, STS de 17 de abril de 2007 más arriba citada[605]: "lo que necesariamente exige una forma que refleje y deje constancia no sólo de su celebración sino de su contenido, que incluso se especifica en sus cláusulas imprescindibles en el propio precepto. Tal exigencia responde a la finalidad de la norma de garantizar que el acceso de terceros a los datos de carácter personal, objeto de tratamiento automatizado, se produzca únicamente en los casos y con las limitaciones legalmente establecidas, plasmándose las condiciones, finalidad y alcance de la cesión de forma que *resulte controlable en su desarrollo y cumplimiento*" (la cursiva es nuestra). El control del desarrollo y del cumplimiento resulta tanto más factible cuanto mayor grado de detalle exista en el contrato[606].

Lo lógico en realidad es que se sigan aplicando muchos de los parámetros que se han descrito anteriormente. Así, si se repasa la propuesta elaborada por el C-SIG-SLA se pude

[605] España. Tribunal Supremo (Sección Sexta de la Sala Tercera de lo Contencioso-Administrativo). Sentencia 2778/2007, de 17 de abril de 2007. Acceso al texto de la Sentencia en el siguiente enlace: http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=503664&links=&optimize=20070531&publicinterface=true

[606] Quizá esta medida no permitirá a IBM cumplir su objetivo de simplificar sus modelos de contratos de servicios de cloud computing que fijaba como regla que todo escrito contractual cuyo objeto contractual se refiera a un servicio de computación en la nube, su extensión no debería exceder de dos páginas. Noticia extractada de ElDerecho.com. 23 de diciembre de 2014. Disponible en web: http://tecnologia.elderecho.com/tecnologia/internet_y_tecnologia/ibm-simplificacion-contratos-servicios_cloud_computing_0_761625006.html

observar que muchas de las referencias que hace el artículo 26 han sido incluidas en la estandarización en el marco del SLA, o bien han sido incluidas dentro de sus guías por las autoridades públicas. Así, a título de ejemplo, en el caso de la autoridad francesa, en el campo de los requisitos legales, se habla no de manera exhaustiva de la necesidad de que consten la localización de los datos, las garantías de seguridad y de confidencialidad, las regulaciones de determinados tipos de datos…etc.[607]; aspectos a los que la autoridad española añade otros como los referidos a la subcontratación o a la portabilidad de los datos[608]. Es decir, las guías y los códigos de conducta en los que se ha venido trabajando para el cloud, cumplen los parámetros del art. 26 RGPD, sin perjuicio de introducir matices o contenidos añadidos.

En línea con la forma en la que dar cumplimiento a las exigencia de contenido contractual, el art. 28.8 RGPD, en aras de la simplificación, ha previsto la posibilidad de que la Comisión Europea o una autoridad de control, aprueben unas cláusulas tipo que puedan servir a efectos tanto de la contratación responsable-encargado (las Directrices para contratos responsable – encargado dictadas por la AGPD en 2017 son un primer paso, pero no son suficientes para la especificidad del cloud), como de la potencial, y casi segura, subcontratación, cuestión esta que trataremos en el apartado oportuno. Estos mecanismos de simplificación también se ponen de manifiesto a través de los códigos de conducta y de los mecanismos de certificación que serán suficientes para acreditar tanto las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas, como para las derivadas de la subcontratación (art. 40. RGPD).

También cabe subrayar, como por otro lado es lógico, que en muchos aspectos las cláusulas que hoy día exige el RGPD, son ya práctica habitual en la contratación en nube. Parece que el nivel de detalle variará en uno u otro caso. Así, no es infrecuente por ejemplo que lo previsto en cuanto a la finalidad del tratamiento sea objeto de una cláusula generalizada. Bien es cierto que en determinadas ocasiones se encuentra establecido en dos cláusulas diferentes dentro de los términos y condiciones de uso o del SLA. Por un lado la referida a seguir las instrucciones del cliente, y por otro lo referido al acceso por parte de terceros. Es además particularmente frecuente que se incluya la limitación del tratamiento de datos a las

[607] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBRTÉS (CNIL). Recommendations for companies planning to use Cloud computing services. Ob. Cit. p. 3, https://www.cnil.fr/sites/default/files/typo/document/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf

[608] AGENCIA ESPAÑOLA DE PROTECCÓN DE DATOS. Guía para clientes que contraten servicios de Computing. Ob. Cit. p. 10.

necesidades derivadas de la prestación del servicio, así como excluir su uso para fines publicitarios[609].

La política de confidencialidad por ejemplo se proyecta en los clásicos contratos (por cuanto a veces se recogen como un contrato distinto) o cláusulas NDA (*Non Disclosure Agreement*). Como señala el INCIBE, lo normal es que se contemplen dos aspectos, que el proveedor no revelará a terceros la información a la que tenga acceso durante la prestación del servicio, y que establecerá las medidas de seguridad necesarias para protegerla (por ejemplo, restringir el acceso a nuestra información exclusivamente a los empleados involucrados, implantar medidas técnicas frente a potenciales atacantes, seguir las pautas legales obligatorias, etc.)[610]. De similar modo, la Guía de la AEPD dice que el proveedor del servicio de cloud debe comprometerse a garantizar la confidencialidad utilizando los datos sólo para los servicios contratados y a dar instrucciones al personal que depende de él para que mantenga la confidencialidad[611].

[609] A título de ejemplo el contrato de aGora. Cloud dice por un lado "*Tratamos los Datos del Cliente de acuerdo con nuestra "Declaración de privacidad". Sujetos a cualquier restricción establecida en la "Declaración de Privacidad", podremos transmitir, almacenar o procesar Datos del Cliente en cualquier país donde nosotros o nuestras Filiales o subcontratistas tengan instalaciones para proporcionar o brindar soporte técnico a los Servicios. Seremos un procesador (o subprocesador) de datos que actuará en su nombre, y usted nos designará para hacer estas cosas con los Datos del Cliente, a modo de prestarle Servicios. Obtendrá todos los consentimientos necesarios de los Usuarios Finales u otros cuya información personal u otros datos se alojarán utilizando los Servicios*"; mientras que señala en otra cláusula distinta: "5. SOLICITUDES DE TERCEROS. *No divulgaremos los Datos del Cliente a un tercero (incluidos la autoridad judicial, otra entidad pública o litigantes en procedimientos civiles; excluidos nuestros subcontratistas), salvo según sus indicaciones o a menos que lo exija la ley. En caso de que un tercero se ponga en contacto con nosotros con una demanda de Datos del Cliente, intentaremos redirigir a dicho tercero a que solicite esos datos directamente a usted. Como parte de este esfuerzo, podemos proporcionar su información de contacto básica al tercero. Si se nos obliga a revelar los Datos del Cliente a un tercero, le notificaremos inmediatamente y* ***le proporcionaremos una copia de la demanda, salvo que esté prohibido por ley.*** *Usted será responsable de responder a las solicitudes de terceros con relación al uso que usted haga de los Servicios, como solicitudes para quitar contenidos en virtud de la Ley Orgánica de Protección de Datos de Carácter Personal de España".* Contrato de Agora.Cloud Versión de agosto de 2014 objeto de acceso en febrero de 2016. https://www.agora-erp.com/es/store/agoracloudagreement

[610] INSTITUTO DE CIBERSEGURIDAD (INCIBE). La ciberseguridad a un clic de tu empresa. Disponible en web: https://www.incibe.es/empresas/que_te_interesa/Contratacion_de_servicios/

[611] AGENCIA ESPAÑOLA DE PROTECCÓN DE DATOS. Guía para clientes que contraten servicios de cloud computing. p.17. Disponible en web: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf

Es igualmente frecuente encontrar cláusulas concernientes la seguridad de los datos[612], la subcontratación, o las denominadas cláusulas de salida, que igualmente vienen siendo incorporadas de manera habitual a las cláusulas de contratos cloud[613].

Sentados estos contenidos contractuales, ya hemos dicho que los mismos en el contrato se van a poder ver sustituidos por una triple vía que gozará de la misma validez jurídica: que se haga constar la adhesión por parte el prestador de servicios cloud a un código de conducta a los que se refiere el RGPD, que se haga constar esa misma adhesión pero a un mecanismo de certificación, o bien la utilización de modelos de cláusulas contractuales desarrolladas por la Comisión o por una autoridad de control. Sobre estas cuestiones nos pronunciaremos en un apartado posterior. No obstante cabe resaltar que la diferencia no será tan pronunciada como pudiera parecer inicialmente. En el caso de las cláusulas modelo será necesario que recojan este tipo de contenido que acabamos de describir y no supondrán sino una vía para facilitar tanto la redacción del contrato en sí mismo como la acreditación de que el mismo se adecúa a las exigencias normativas. Además es importante subrayar que en el caso concreto de los códigos de conducta y de los mecanismos de certificación, no son suficientes para algunos de los elementos a los que nos hemos referidos. El RGPD habla de que la adhesión sirve para demostrar la concurrencia de las garantías exigidas. Estas por tanto abarcaran cuestiones susceptibles de estandarización como la vinculación al fin del tratamiento fijado por el cliente, la política de confidencialidad del prestador, la colaboración en el ejercicio de sus derechos por los interesados, o sus medidas de seguridad. Pero no podrán sustituir otros elementos que son esencialmente contractuales por ser necesaria la concurrencia de la voluntad concreta del cliente (se habla de elección por el responsable), caso de las opciones

[612] A título de ejemplo, el contrato de Locategy S.L. dice en este punto: "*Locategy SL manifiesta estar al corriente en la implantación de las medidas de seguridad de nivel básico previstas en los artículos 88 a 94 y 105 a 108 del Real Decreto 1720/2007 y, expresamente, disponer de un documento de seguridad actualizado, haber definido perfiles de usuarios y establecido los correspondientes controles para el acceso a datos de carácter personal y medidas suficientes para la identificación y autenticación del Usuario, así como disponer de los preceptivos procedimientos de gestión de incidencias, gestión de soportes y documentación (incluidos criterios de archivo, almacenamiento y custodia de ficheros no automatizados), realización de copias de respaldo, y recuperación de datos. Locategy SL se obliga asimismo a adoptar las medidas de seguridad adicionales que pudieran ser exigidas por la normativa vigente, en el supuesto de existir un tratamiento de datos de carácter personal de nivel superior*", Contrato de Locategy SL. Objeto de acceso en febrero de 2016 https://locategy.com/legal-info?lang=es

[613] De nuevo como ejemplo, podemos señalar cómo las condiciones generales de CloudVPS (de la empresa SVT) contemplan: "*Una vez que se finalizado el contrato, bien por extinción del plazo, bien por cualquiera de las causas previstas de resolución, SVT CLOUD SERVICES procederá al borrado inmediato de la cuenta del CLIENTE y de todos los datos alojados en sus servidores y vinculados a dicha cuenta a lo que el CLIENTE presta su consentimiento de forma expresa renunciando a reclamar ningún daño o perjuicio contra SVT CLOUD SERVICES*".

de salida; o bien, aunque aquí con mayores matices, por estar condicionadas por la prestación del servicio concreto, caso de la subcontratación.

Como una consecuencia lógica de estos compromisos que adquiere el prestador del servicio, será necesario que en el contrato se haga constar de una manera concreta: la finalidad del tratamiento, las medidas de seguridad, los servicios que se subcontratan, el protocolo o la forma en que se facilitará la satisfacción de los requerimientos de los interesados, o el mecanismo referido la cláusula de salida concreta; sin perjuicio de que algunos de los elementos hayan ya sido objeto de descripción en el contenido propio del SLA.

Como conclusión cabe señalar que el contrato entre el prestador de servicios cloud y el cliente será un contrato de prestación de servicios que deberá hacerse constar por escrito; que responderá habitualmente a un esquema de adhesión; con una estructura dual de contrato marco y anexos, siendo dentro de estos el SLA y, en su caso, el PLA, los más relevantes. En el apartado o cláusula específica de la protección de datos, se deberá incluir un contenido mínimo recogido en el RGPD, sin perjuicio de su eventual sustitución parcial, en el plano de las garantías, por las fórmulas de adhesión a mecanismos de estandarización.

Pero la importancia del contrato no viene dada exclusivamente en cuanto que instrumento generador de las obligaciones de las partes, sino que en el ámbito del cloud juega un papel fundamental como elemento de compliance, de garantía para el cliente y frente a terceros, tanto autoridades como interesados. El contrato, y el alto grado de detalle exigido, favorecen al cliente/responsable, pues si bien es cierto que este no queda exento de responsabilidad, ello no obsta para que el contrato sea una extensión de la normativa que garantiza en cierta medida una protección de dicho responsable. En el ámbito cloud, además, resulta particularmente conveniente el recurso a los códigos de conducta y en este punto es digno de destacar, como ya se ha dejado ver a lo largo del texto, el trabajo realizado por la industria en el grupo constituido por los proveedores y amparado por la Comisión Europea. Si este código culmina, puede, sin duda, convertirse en un estándar normalizado, bajo el paraguas del art. 40 RGPD, que dote de seguridad jurídica al proveedor, de garantía al cliente, y de protección a los interesados que ponen sus datos en manos de los anteriores. La promoción de estos sistemas interesados constituye una obligación, ex. art. 40.1 RGPD, de los Estados miembros, las autoridades de control, el Comité y la Comisión. La asimetría del cloud, incluso en el entorno B2B que nos ocupa, lo destaca como un elemento llamado a jugar un papel creciente.

Idénticas reflexiones cabría realizar respecto de los modelos de cláusulas, que tan importante pape han jugado por ejemplo en las transferencias internacionales. Lo cierto es que a nuestro juicio no es tanta la diferencia en el plano material entre un código de conducta o el modelo de cláusulas. Ambos instrumentos servirán, no solo a los efectos de demostrar algunas exigencias normativas del RGPD, sino que contribuirán a la seguridad jurídica y a la competitividad económica. Su procedimiento, más sencillo que el normativo, les lleva a jugar un papel clave en el mundo jurídico-tecnológico y el cloud no es sino un ejemplo.

4 El ejercicio de los derechos por los interesados

4.1 Introducción

Como proyección específica del derecho fundamental a la protección de datos y como manifestación de su contenido esencial, se encuentran los derechos que corresponden a cada uno de los interesados. De hecho la regulación de la protección de datos es particularmente incisiva en los derechos que otorga a los interesados y las consiguientes obligaciones que impone a los responsables y a los encargados[614], por lo que resulta necesario observar, una vez más, cómo se compadece el tratamiento jurídico con el hecho de que la condición de encargado venga asumida por un proveedor de servicios en nube y si resulta adecuado para el papel que a este le corresponde.

Tradicionalmente estos derechos se conocen como derechos ARCO (acrónimo que responde a los derechos de acceso, rectificación, cancelación y oposición). Estos se encuentran recogidos en la Directiva 95/46. En concreto, el derecho de acceso (art. 12); los derechos de rectificación, supresión o bloqueo (art. 12.b); y oposición (art. 14). Por su parte, la LOPD los contempla igualmente: acceso (art. 15), oposición (art. 13), rectificación y cancelación (art. 16). Tal es la importancia de estos derechos que el Grupo de Trabajo del art. 29 señaló en 2010 que "el papel primero y primordial del concepto de responsable del tratamiento es determinar quién debe asumir la responsabilidad del cumplimiento de las normas sobre protección de datos y de qué manera los interesados pueden ejercer sus derechos en la práctica"[615].

---

[614] PEARSON, S. y CHARLESWORTH, A. Developing accountability-based solutions for data privacy in the cloud*";* en FRIEDWALD, M. y POHORYLES, R.J. (Eds.). *Privacy and Security in the Digital Age: Privacy in the Age of Super-Technologies.* Routledge. 2016. p. 7-35.

[615] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento. Disponible en web: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_es.pdf

El caso del RGPD es más llamativo por cuanto no solamente ha mantenido los derechos tradicionales que emanan del derecho a la protección de datos, sino que ha añadido algún otro. Efectivamente, se mantiene el derecho de acceso (art. 15), el derecho de rectificación (art. 16), el derecho de supresión (art. 17) y el derecho de oposición (art. 21). No obstante como derechos autónomos o más bien como vertientes de algunos de los derechos anteriores, se han incluido algunos nuevos como el derecho al olvido (art. 17), el derecho a la limitación del tratamiento (art. 18), el derecho a la portabilidad (art. 20) y el derecho de oposición a las decisiones individuales automatizadas, incluida la elaboración de perfiles (art. 22), de particular importancia en entornos de tratamiento masivo de datos *(Big Data*) y de inteligencia artificial. No nos corresponde ahora entrar en si el derecho al olvido tiene autonomía propia o es una proyección del derecho supresión, si lo mismo cabe decir del derecho a la limitación respecto del derecho de oposición o si este también tiene como proyección el mencionado en el art. 22 RGPD respecto de las decisiones automatizadas, y en particular la elaboración de perfiles. Apuntamos que a nuestro juicio la sustantividad propia solamente cabe reconocerla respecto al derecho a la portabilidad de los datos, al que dedicaremos un apartado específico en este capítulo por su particular importancia en el entorno cloud. A todos ellos habría que unir el derecho a la información (arts. 13 y 14) que si bien recibe esta denominación de manera muy generalizada, cabría debatir si se trata más de una obligación por parte del responsable que un derecho por parte el titular de los datos y ello si consideramos que es algo que está llamado a hacer el responsable sin necesidad de requerimiento alguno por parte de los interesados. No obstante, y a pesar de la nomenclatura utilizada en el RGDP lo cierto es que autoridades y jurisprudencia lo vienen considerando un auténtico derecho. Así se ha reconocido por ejemplo en la Sentencia del Tribunal Constitucional 29/2013, de 11 de febrero de 2013[616], o en la Sentencia de la Audiencia Nacional de 9 de septiembre de 2004[617], y en general así lo viene catalogando de manera clara la Agencia Española de Protección de Datos a la hora de enumerar los derechos de los interesados[618].

---

[616] España. Tribunal Constitucional (Sala Primera). Sentencia 29/2013, de 11 de febrero. Disponible en web: http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_constitucional/common/pdfs/SENTENCIA_29-2013_de_11_de_febrero__de_2013.pdf

[617] España. Audiencia Nacional (Sala de lo Contencioso-Administrativo, sección primera). Sentencia de 9 de septiembre de 2004. Disponible en web: http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/audiencia_nacional/common/pdfs/Sentencia-Audiencia-Nacional-09-06-2004.pdf

[618] https://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/informacion-ides-idphp.php

¿Qué obligaciones tiene el cliente de la nube en cuanto que responsable y el proveedor en cuanto que encargado cuando un titular de derechos ejerce alguno de los anteriormente citados? Estamos ante una cuestión de gran relevancia y prueba de ello es cómo la garantía de la satisfacción de estos derechos o más bien el incumplimiento de los mismos ha recibido una previsión sancionadora elevada que conforme al art. 83.5.b) RGPD podrá llegar a multas administrativas de 20 000 000 EUR como máximo o de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior.

Hacer realidad estos derechos corresponde básicamente al responsable del tratamiento, con independencia, de nuevo, de cuál sea el tamaño empresarial del cliente y proveedor. Así figura en los arts. 15 a 22. Es más, y como se ha visto anteriormente, forma parte del contenido contractual. En concreto el art. 28.3.e) RGPD obliga al encargado a asistir al responsable, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados a través de medidas técnicas y organizativas.

Por lo tanto el proveedor ha de asistir ¿Y en qué se concreta la asistencia que ha de prestar el proveedor? ¿Qué dificultades específicas se plantean en el ámbito de la computación en nube? La ENISA, en su informe sobre los riesgos derivados del cloud computing apuntaba que uno de ellos podría ser el derivado de los problemas de gestión de los derechos de acceso de los interesados derivados de la inadecuación de los medios puestos a disposición por el proveedor[619]. A ello añade, en el plano estrictamente tecnológico, que uno de los retos va a ser la implantación de los derechos de acceso, rectificación, cancelación y oposición debido a que la naturaleza distribuida puede hacer más difícil la aplicación de los mismos[620].

El Grupo de Trabajo del art. 29 ha señalado dentro de los riesgos de la computación en nube, y más concretamente de la falta de control, es la falta de posibilidad de intervención (derechos de los interesados): un proveedor no podrá aportar las medidas e instrumentos necesarios para ayudar al responsable del tratamiento a gestionar los datos en términos de,

---

[619] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. Recommendations for companies planning to use Cloud computing services. Ob. Cit. p. 4.

[620] IOKONOMHOU, D. (ENISA). Impact of the proposed data protection regulation on cloud computing. *Cybersecurity & Privacy Innovation Forum 2015 (CSP Forum)*. 28-29 April, 2015. Disponible en web: https://www.cspforum.eu/graphics/2015/speakersfiles/1.%20demosthenes%20Ikonomou_Cloud_DataProtection_CSP2015_DI.pdf

por ejemplo, acceso, supresión o corrección[621]; argumento reproducido por la AEPD en su Informe 0464/2012[622].

Las autoridades nacionales de protección de datos han llamado también la atención sobre esta cuestión, si bien de manera sucinta. La autoridad británica ha recordado que el cliente de la nube debe asegurarse que moverse a un servicio cloud permite en todo caso a los interesados ejercer sus derechos[623]. También la autoridad alemana subraya la necesidad de que los clientes se aseguren de que el proveedor respeta los derechos de los interesados[624]. La autoridad francesa, con mayor detalle, recuerda que el hecho de que los datos puedan estar en diferentes servidores ubicados en distintos países puede hacer más complicado para los interesados el ejercicio de sus derechos, y por tanto es necesario asegurar que el proveedor y el cliente estén dando las suficientes garantías para permitir a los interesados el ejercicio de sus derechos. A pesar de esta afirmación que podría situar la responsabilidad de uno y otro en el mismo plano, lo cierto es que matiza que la responsabilidad es del cliente (con la asistencia del proveedor)[625]. La autoridad española ha manifestado a su vez, en la misma línea, que el proveedor de cloud debe garantizar su cooperación y las herramientas adecuadas para facilitar la atención de dichos derechos[626].

También fuera de las fronteras comunitarias, las autoridades de protección de datos de las islas de Jersey y de Guernsey, señalan como uno de los riesgos principales el hecho de que un proveedor pueda no facilitar las medidas necesarias y las herramientas para asistir al cliente en la gestión de los datos en lo concerniente al acceso, la supresión, la rectificación…[627]. Igualmente las autoridades suizas señalan como uno de los riesgos específicos del cloud que el cliente, en cuanto que responsable de los datos, no sabe exactamente dónde los datos están siendo almacenados y tratados. Frecuentemente no

---

[621] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 05/2012 sobre la computación en nube. ob. cit. p. 7.

[622] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Informe 0464/2012. Disponible en web: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2012-0464_Contrataci-oo-n-de-servicio-de-cloud-computing-por-cl-ii-nica-m-ee-dica.pdf

[623] INFORMATION COMMISSIONER'S OFFICE. Guidance on the use of cloud computing. Ob. Cit. p. 21.

[624] DIE DATENSCHUTZBEUFRAGTN ES BUNDES UND DER LÄNDER. Orientierungshilfe – Cloud Computing. 9 de octubre de 2014. Disponible en web : https://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf

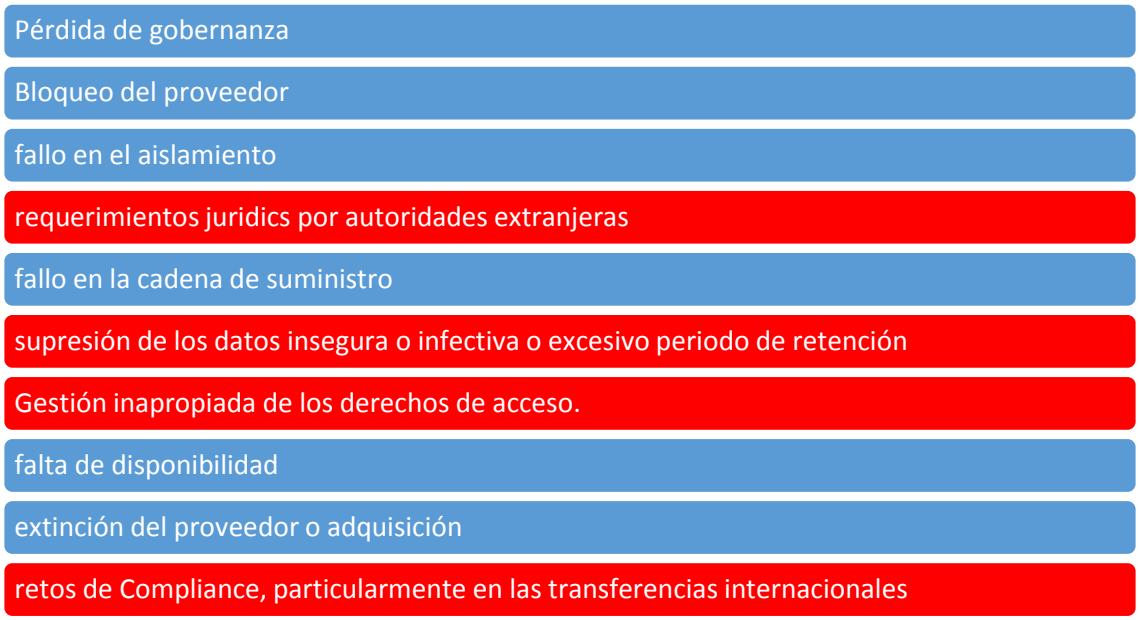
[625] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. Recommendations for companies planning to use Cloud computing services. Ob. Cit. p. 6.

[626] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía para clientes que contraten servicios de Cloud Computing. Ob. Cit. p. 18.

[627] INFORMATION COMMISSIONER (JERSEY) AND DATA PROTECTION COMMISSIONER (GUERNSEY). Cloud Computing A guide for data controllers. abril de 2016. Disponible en web: https://dataci.je/wp-content/uploads/2016/04/Cloud-Computing_Apr16.pdf

sabe si hay subencargados implicados y si hay una protección suficiente, lo que conlleva que no pueda garantizar algunos requisitos: seguridad de los datos, *derecho de acceso* o supresión de los datos[628].

La autoridad francesa por su parte ha señalado, como se observa en este cuadro, los diez riesgos con mayor relevancia para la protección de datos en el entorno del cloud computing:



Fuente: CNIL[629]. En rojo los de mayor impacto en la protección de datos según la autoridad francesa y entre los que se incluyen los derechos ARCO

Desde el punto de vista de la industria, y tal y como ya se ha presentado en el apartado anterior, dentro de las directrices de los contratos se sitúa la denominada *data intervenability,* que se define precisamente como la capacidad del proveedor de asistir al cliente de la nube a la hora de facilitar el ejercicio de los derechos de los interesados. En el ya citado código de conducta, y partiendo lógicamente de la responsabilidad por parte del cliente, se señala que la cooperación o asistencia necesaria y de buena fe se tiene que dar. En este sentido apunta que el proveedor, o bien facilitará a sus clientes la posibilidad de rectificar, suprimir o bloquear

[628] FEDERAL DATA PROTECTION INFORMATION COMMISSIONER. Guide to cloud computing. Disponible en web: https://www.edoeb.admin.ch/datenschutz/00626/00876/01203/index.html?lang=en
[629] LE GRAND, G. Cloud computing and personal data protection. *CSA Congress EMEA*. noviembre de 2015. Disponible en web: https://csacongress.org/wp-content/uploads/2015/11/csa-congress-emea-2015_-_Gwendal-Grand.pdf

los datos personales en la nube, o ejecutará dichas actuaciones en nombre de sus clientes. Cuestión a tratar con posterioridad será la obligación del proveedor de asegurarse de que cualquiera de los subencargados asegure un nivel equivalente de cooperación[630].

En la misma línea *CloudWatch* señala que cuando lea el contrato de cloud computing, el cliente deberá verificar que el proveedor garantiza una total cooperación a la hora de asegurar un ejercicio efectivo y sencillo de los derechos de los interesados, incluyendo también aquellos casos en los que los datos son tratados por subencargados[631], cuestión esta que trataremos separadamente en otra parte de este capítulo. Descendiendo a la realidad práctica de la industria, y manteniendo el marco de este estudio, es decir, cuando nos encontramos con un proveedor como encargado del tratamiento[632], es frecuente que el proveedor adopte medidas técnicas y organizativas para satisfacer por ejemplo el derecho de acceso, como son Privacy dashboard OASIS XACML, ITU-T X.1142[633].

4.2 Acercamiento a los derechos específicos.

4.2.1 La obligación de informar.

Entrando ya en el contenido concreto del derecho a la información, se distingue en función de si los datos se obtienen o no de los interesados. En el primer caso, el art. 13 RGPD dispone que se deberá facilitar la siguiente información: la identidad y los datos de contacto del responsable o de su representante; los datos de contacto del delegado de protección de datos; los fines del tratamiento y la base jurídica del mismo; en su caso, los intereses legítimos del responsable o de un tercero; los destinatarios o las categorías de destinatarios de los datos personales; la intención del responsable de transferir datos internacionalmente y la garantía adecuada en la que se basa; el plazo durante el cual se conservarán los datos personales o los criterios utilizados para determinarlo; la existencia de los derechos de los

---

[630] C-SIG SUB-GROUP ON THE DATA PROTECTION CODE OF CONDUCT. Code of Conduct for Cloud Service Providers. Ob. Cit. p. 22.

[631] CLOUDWATCHHUB. The CloudWATCH Legal Guide to the Cloud for SMEs. p. 3. Disponible en web: http://www.cloudwatchhub.eu/sites/default/files/CloudWATCH_Legal-guide-to-the-cloud.pdf

[632] El estudio por ejemplo elaborado por *CloudLegalProject* de la *Queen Mary University* se centra en hasta veinte proveedores de servicios cloud, pero sin embargo la mayoría de ellos actúan como responsables del tratamiento y consiguientemente su forma de satisfacer los derechos de los interesados no nos resulta válida a nuestros efectos. No obstante, si se quiere profundizar, se encuentra en: KAMAINOU, D., MILLARD, C. y KUAN HON, W. Privacy in the Clouds: an Empirical Study of the Terms of Service and Privacy Policies of 20 Cloud Service Providers. *Queen Mary University of London. School of Law Legal Studies Research Paper No 209/2015*. 71 p. Particularmente páginas 44 a 50. Disponible en web: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2646447

[633] ITU-T. Technology Watch Report. Privacy in Cloud Computing. marzo de 2012. Disponible en web: https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf

interesados debidamente enumerados; en caso de que el tratamiento se base en el consentimiento, la existencia del derecho a retirarlo; el derecho a presentar una reclamación ante una autoridad de control; y si la comunicación de datos es un requisito legal o contractual, o necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos y está informado de las posibles consecuencias de que no facilitarlos; la existencia de decisiones automatizas, incluida la elaboración de perfiles, y la información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado. Muy similar será la información en el caso de que la información no se haya obtenido del interesado, añadiendo la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público. En todo caso, cabe subrayar que en este último supuesto el derecho a la información queda vacío de contenido cuando concurra algunas de las circunstancias previstas en el art. 14.5 RGPD: el interesado ya disponga de la información; la comunicación resulte imposible o suponga un esfuerzo desproporcionado, o pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En estos últimos supuestos, el responsable está obligado a adoptar medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información. También quedará vacío de contenido el derecho a la información cuando la obtención o la comunicación esté expresamente establecida por normativa comunitaria o nacional que se aplique al responsable y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o cuando esas mismas fuentes jurídicas –incluyendo las normas estatutarias– señalen que los datos deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional. En realidad, como sucede en otros ámbitos, el RGPD, como es lógico también por la fuente del Derecho a la que se ha recurrido, ha ampliado la información que se ha de facilitar.

A los efectos que nos ocupan, y más allá del contenido concreto de este derecho, en el ámbito específico del cloud computing se trata de un supuesto en el que no es necesaria la colaboración del proveedor de servicios en nube. Estamos ante el presupuesto ontológico de cualquiera de los derechos, el momento de recopilación de los datos en el que no ha entrado en juego el acceso a los mismos por parte del encargado del tratamiento. Este derecho por tanto solamente puede ser satisfecho por el responsable o cliente, sin que quepa exigir obligación alguna al proveedor. La labor de asistencia que compete al proveedor en tanto que encargado, no es ni necesaria, y ni siquiera pertinente.

Cabe mencionar por último en este punto la forma de satisfacer el derecho a la información previsto en los arts. 13 y 14, por cuanto el apartado 7 del art. 12 RGPD permite la posibilidad de que se haga con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto, siendo necesario que cuando se facilite en formato electrónico los referidos iconos sean legibles mecánicamente. Se trata en todo caso de una cuestión abierta por cuanto no toda la información es susceptible de ser facilitada por esta última vía. Así parece confirmarlo el art. 12.8 al señalar que le corresponderá a la Comisión Europea dictar los oportunos actos delegados tanto para especificar la información que se ha de presentar a través de iconos (de lo que cabe deducir que no toda) y los procedimientos para proporcionar iconos normalizados. En realidad estamos ante un elemento destinado a combinar el detalle que exige el RGPD con la necesidad de un lenguaje claro y sencillo (art. 12.1); al igual que la distribución de la información por capas que han recomendado las autoridades nacionales de protección de datos: con una información básica en un primer nivel, de forma resumida, en el mismo momento y en el mismo medio en que se recojan los datos; y una información adicional en un segundo nivel, donde se presentarán detalladamente el resto de las informaciones[634].

4.2.2 El derecho de acceso

El derecho de acceso tiene una triple proyección: la confirmación o no de la existencia del tratamiento, el derecho al acceso a los datos en sí mismo y el derecho de acceso a una determinada información. Procede por tanto analizar cada una de estas vertientes.

- Parece razonable que el cliente de los servicios en nube no necesita del proveedor para satisfacer la primera versión de este derecho, esto es, la confirmación del tratamiento, sin perjuicio de que nada impediría la posibilidad de que el proveedor lo hiciera. El interesado se dirigirá al responsable del tratamiento y este responderá afirmativa o negativamente según proceda, siendo por tanto presupuesto de las otras dos vertientes y de cualesquiera otros derechos de los tratados en la normativa; sin que en todo caso el ejercicio de uno de ellos se pueda poner como requisito para el ejercicio de cualquier otro (art. 24.1 in fine ROPD). Cabe subrayar que, aunque bajo

[634] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía para el cumplimiento del deber de informar. 2017. Disponible en web: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/modeloclausulainformativa.pdf

el epígrafe “derecho de acceso”, el RGPD, en su art. 15.1, parece extraer esta facultad del derecho de acceso en sí mismo por cuanto en la redacción señala: “*El interesado tendrá derecho a obtener del responsable del tratamiento* ***confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso*** *a los datos personales y a la siguiente información*”. Podríamos por tanto decir que estamos ante un derecho autónomo, el derecho a la confirmación del tratamiento.

Respecto a la forma en la que ejercer este derecho, bastará con recurrir a cualquiera de los medios que la normativa actual contempla (art. 28.1 RODP): visualización en pantalla; escrito, copia o fotocopia remitida por correo, certificado o no; telecopia; correo electrónico u otros sistemas de comunicaciones 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.

- En cuanto al acceso a los datos en sí mismo, la presencia de un encargado del tratamiento conlleva que su participación –o asistencia en terminología legal– sea necesaria. Será el encargado, en cuanto que persona que está procediendo al tratamiento de los datos por cuenta del responsable, quien deba facilitar los datos a este o, en caso de que el interesado se dirija directamente al encargado, y así se hubiera contemplado en el contrato, que sea el propio encargado el que lo satisfaga directamente. Además las notas particulares de la nube marcadas por elasticidad, ubicuidad, dinamismo en el alojamiento de los datos, sofisticación tecnológica en muchas ocasiones, hará inevitable en la práctica que esto sea así. En todo caso, y como proyección de los roles en general que uno y otro asumen, no se debe olvidar que es al responsable al que corresponde esa obligación frente al interesado (art. 15.3 RGDP), sin perjuicio de lo que posteriormente se señalará. El RGPD ha primado la satisfacción del derecho de acceso a través de medios electrónicos, cuando el interesado presente la solicitud por dichos medios, salvo que solicite que se facilite de otro modo. De hecho, como señala el Considerando 63 del RGPD “*Si es posible, el responsable del tratamiento debe estar facultado para facilitar acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales*”. El único límite a esta vertiente del derecho a la copia será el fijado por los derechos

de terceros. Además cabe subrayar que será gratuita, pudiendo aplicar un coste para cualquier otra copia ulterior.

- La última vertiente tampoco exige de la colaboración necesaria por parte del proveedor de servicios en nube por cuanto se limita a facilitar una determinada información que viene expresamente recogida en la norma y de hecho, como se ha apuntado en el derecho a la información, es el responsable el único que puede satisfacerlo en partes de su contenido como por ejemplo los fines del tratamiento. En concreto, el art. 15.1 recoge que el ejercicio del derecho de acceso conlleva que el responsable facilite la siguiente información: los fines del tratamiento; las categorías de datos personales de que se trate; los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales; de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo; la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento; el derecho a presentar una reclamación ante una autoridad de control; cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen; la existencia de decisiones automatizadas, incluida la elaboración de perfiles, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado. A esta será necesario añadir que en caso de que se hayan transferido datos personales a un tercer país o a una organización internacional, el interesado deberá ser informado de las garantías adecuadas relativas a la transferencia.

4.2.3 Derecho de rectificación, derecho de supresión y derecho al olvido.

En lo que concierne al derecho de rectificación, el RGPD no ha introducido novedad alguna en cuanto a que mantiene la doble vertiente de que se modifiquen los datos cuando los mismos resulten inexactos y que se completen cuando resulten incompletos (art. 16

RGPD)[635]. En este caso, y sin perjuicio de lo que posteriormente se señalará, el prestador de servicios en nube deberá limitarse a seguir las instrucciones del responsable en cuanto a proceder a modificar o completar los mismos. En caso de que el derecho se ejerciera directamente ante el proveedor, este deberá comunicarlo al responsable y seguir las instrucciones que el mismo le señalara, asistiéndole lógicamente, en la satisfacción concreta del derecho. Parece lógico que si quien ha recogido los datos es el responsable, sea este quien, a la vista del ejercicio del derecho, dicte las correspondientes instrucciones. Cierto es que en la normativa todavía aplicable se contempla (ex. art. 26 ROPD) que el derecho de rectificación debe ser atendido, por cuenta del responsable, por parte del encargado, pero a nuestro juicio dicha atención se ve cumplida al solicitar de las referidas instrucciones y la posterior satisfacción material en su caso.

Mayor importancia ha tenido el derecho de supresión, fundamentalmente tras verse aumentado su campo de actuación con el denominado derecho al olvido. En el RGPD este derecho se ha concretado en la obligación del responsable de suprimir, sin dilación indebida, los datos del interesado, cuando concurra alguna de las siguientes circunstancias: pérdida de calidad de los datos; retirada del consentimiento para su tratamiento y ausencia de otro fundamento para mantenerlo; tratamiento ilícito; obligación legal; o bien cuando los datos se hayan obtenido en relación con la oferta de servicios de la sociedad de la información a niños.

El derecho al olvido propiamente dicho se encuentra en realidad reflejado en el apartado 2 del propio art. 17 RGPD donde se dice que cuando el cliente haya hecho públicos los datos personales, adoptará medidas razonables para informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos. El deber del responsable del tratamiento –del cliente– es adoptar dichas medidas en función de dos criterios: la tecnología y el coste.

Los anteriores derechos, el derecho a la supresión y el derecho al olvido, se pueden ver vaciados de contenido si se aplican algunos de los siguientes límites que contempla el art.

[635] De hecho la redacción de este precepto mejora la prevista en la legislación española. El art. 31.1 ROPD señala que el derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompleto, teniendo lógica la modificación respecto a lo primero (la inexactitud), pero no frente a la segunda (el carácter incompleto). La redacción del art. 16 refleja claramente la doble vertiente de manera mucho más atinada: "*El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional".*

17.3 RGPD: el derecho a la libertad de expresión e información; el cumplimiento de una obligación legal, o el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable; por razones de salud pública; con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos; o para la formulación, el ejercicio o la defensa de reclamaciones.

En el ejercicio del derecho de supresión, la colaboración por parte del prestador se hace absolutamente imprescindible. Tal y como se tratará con detalle cuando se analice la denominada "cláusula de salida", se trata de uno de los aspectos críticos del *cloud computing*. La continua movilidad de los datos, consustancial al modelo de computación en nube; la potencial cadena de subcontrataciones; la complejidad de los entornos tecnológicos y otras muchas variables, hacen que nos encontremos ante uno de los derechos por excelencia en el entorno cloud. Como ha señalado el Grupo de Trabajo del art. 29, teniendo en cuenta que los datos pueden mantenerse de manera redundante en diferentes servidores en diferentes ubicaciones, debe asegurarse que en cada uno de ellos los datos son eliminados de manera irreversible (por ejemplo versiones previas, archivos temporales e incluso fragmentos de archivos)[636], y ello es algo que solo el proveedor, en su caso con los correspondientes subencargados, puede satisfacer[637].

Como ha apuntado igualmente el referido Grupo de Trabajo, un borrador seguro de los datos requiere que, o bien se destruyan los medios de almacenamiento, o se desmagneticen o que sean borrados de una manera efectiva sobrescribiendo los datos. Para esto último existen herramientas de software que sobrescriben los datos en muchas ocasiones con especificaciones reconocidas[638]. En todo caso, la exigencia de un certificado de destrucción de los datos por parte del encargado del tratamiento parece un mecanismo razonable para

[636] ARTICLE 29 WORKING GROUP. Opinion 5/2012 on Cloud Computing. Ob. Cit. p. 12.
[637] POHLMANN, N., REIMER, H. SCHNEIDER, W. *ISSE 2010 Securing Electronic Business Processes* Springer Science & Business Media. 2011. 213 p.
[638] *Idem.* p. 171. En la misma línea también la Unión Internacional de Telecomunicaciones en su documento "P*rivacy in Cloud Computing*", 2012, en cuya página 4 distingue entre por un lado las PET que se pueden considerar como aquellas tecnologías que reducen el riesgo de contravenir la regulación y los principios de privacidad, minimizan la cantidad de datos conservados respecto de los interesados y permiten a los interesados mantener el control de la información sobre ellos en todo momento; y por otro lado las TET (*Transparency enhancing tools*) que facilitan a los usuarios información respecto a las políticas de privacidad o garantizan a los interesados el acceso online a sus datos personales. UIT. Privacy in Cloud Computing. 2012. Disponible en web: https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf

satisfacer tanto los derechos del cliente como la potencial demostración de satisfacción del derecho a la supresión ante el interesado.

4.2.4 Derecho a la limitación del tratamiento, derecho de oposición, y decisiones individuales automatizadas.

Otro derecho que contempla el RGPD es el derecho a la limitación del tratamiento que le corresponde al interesado cuando concurren determinados presupuestos materiales y condicionantes temporales: cuando impugne la exactitud de los datos, durante un plazo que permita al responsable verificarlo; cuando sea ilícito y el interesado se oponga a la supresión; cuando el responsable no los necesite, pero sí el interesado para el ejercicio de defensa; cuando haya ejercido el derecho de oposición mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado. Cuando esto se produzca y dada la implicación directa que tiene sobre el tratamiento en sí mismo, será necesaria una comunicación directa y fehaciente al encargado por cuanto, más allá de la conservación en sí misma, solo podrán tratarse por una serie de motivos tasados: consentimiento del interesado; formulación, ejercicio o defensa de reclamaciones, o la protección de los derechos de otra persona física o jurídica, o por razones de interés público importante de la Unión o de un determinado Estado miembro (art. 18.2 RGPD).

En la misma línea se sitúa el tradicional derecho de oposición, que le permite al interesado negarse a que se traten sus datos cuando la causa de este sea el interés público o el interés legítimo (art. 21.1 RGPD), salvo que el cliente/responsable acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, derechos y libertades del interesado, o para el ejercicio de reclamaciones (art. 21.1 RGDP *in fine*). A muy similares características responde la posibilidad del interesado de oponerse a que se tomen decisiones que le afecten basadas exclusivamente en el tratamiento automatizado (art. 22.1 RGPD). Este último será un derecho que no concurra cuando exista la necesidad de dicho tratamiento para la celebración o ejecución de un contrato, se encuentre autorizado por el Derecho de la UE o de un Estado miembro, o bien haya concurrido –lógicamente– el consentimiento explícito del interesado (art. 22.2 RGPD). En todo caso, nunca podrán estar basadas en categorías especiales de datos, y cuando concurran las causas justificativas contractual o de consentimiento, se deben adoptar medidas que incluyan –como mínimo– el derecho a obtener la intervención humana por parte del responsable.

4.3 Elementos comunes a los derechos del interesado.

Hasta ahora se ha planteado cómo la satisfacción jurídica de los derechos puede darse por el responsable directamente o bien por el encargado actuando, como si una fase más del tratamiento fuera, en nombre del responsable; y todo ello sin perjuicio de que, como se ha ido igualmente viendo, la cooperación material por parte del encargado, y más en la computación en nube, se presenta como absolutamente necesaria en algunos de los casos.

Hoy día, la todavía aplicable normativa española, recoge la posibilidad de que los derechos anteriormente mencionados se ejerzan directamente ante el encargado, en nuestro caso ante el proveedor (art. 26 ROPD). La filosofía subyacente a la relación interesado-responsable se pone de manifiesto cuando esto ocurre, por cuanto el referido precepto señala que la primera actuación por parte del proveedor deberá ser la de dar traslado de la solicitud al responsable, a fin de que por él mismo se resuelva. Sin embargo, el matiz que se introduce tiene particular relevancia ya que se dice que ello será así, "a menos que en la relación existente con el responsable del tratamiento se prevea precisamente que el encargado atenderá, por cuenta del responsable, las solicitudes de ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación u oposición".

Es cierto que el contenido del contrato en el RGPD habla de asistir y cooperar, y que no hay una previsión expresa de que esta opción exista para los interesados. No obstante, una interpretación lógica nos lleva a pensar que la principal vía de cooperación o asistencia puede ser precisamente esta satisfacción directa de los derechos bajo el conocimiento previo del responsable del fichero. La previsión en el contrato de la forma en la que se van a satisfacer estos derechos adquiere una particular relevancia cuando se produce este almacenamiento a distancia. En concreto, como señala Marit Hansen, el cliente debe verificar por un lado que el proveedor no impone obstáculos técnicos u organizativos a los derechos de los interesados y, por otro lado, debe comprobar si el proveedor garantiza la portabilidad de los datos y de qué manera lo hace[639]. Es aconsejable que los términos de la cooperación entre las partes se especifiquen en el contrato[640].

---

[639] HANSEN, M. The Art of Intervenability for Privacy Engineering. *Workshop "Data Protection, Privacy, and Transparency*" (DPPT'15). Hamburg. 26 de mayo de 2015. Disponible en web: https://www.datenschutzzentrum.de/uploads/vortraege/20150226_ArtOfIntervenability_Hansen_final.pdf

[640] [640] POHLMANN, N., REIMER, H. SCHNEIDER, W. *ISSE 2010 Securing Electronic Business Processes*. Ob. Cit. p. 171.

A juicio de la autoridad británica, cuando un interesado ejerza por ejemplo su derecho de acceso, el responsable podrá requerir al encargado para que le facilite los datos de tal manera que el cliente satisfaga el derecho por sí mismo, o bien dictar instrucciones al proveedor para que pueda ocuparse de ese requerimiento. Sin embargo considera que esto último solo es factible si es un requerimiento ordinario. El cliente habrá de especificar al encargado cómo gestionar ese requerimiento, por ejemplo estableciendo si hay determinado tipo de categorías que deberán ser ocultadas. Sin embargo –continúa la autoridad británica– si es un requerimiento de acceso menos ordinario e implica un trabajo para decidir caso por caso si una particular excepción se aplica, entonces solamente el responsable puede gestionarlo debido al componente valorativo que pueda tener que aplicarse a las excepciones al acceso[641]. Las autoridades de Jersey y Guernsey también contemplan la necesidad de que, en aras del principio de seguridad jurídica, el contrato incluya la obligación del proveedor de apoyar al cliente a la hora de facilitar el ejercicio de los derechos de acceso, rectificación o supresión[642]. En todo caso, se debe subrayar, como recordaba el Supervisor Europeo de Protección de Datos, que aunque el proveedor deba cooperar con el responsable de cara a cumplir con la obligación de este de atender a los derechos de los interesados y de asistir al responsable en asegurar el cumplimiento con los requisitos de seguridad, las notificaciones de quiebra, la evaluación de impacto de la privacidad, la responsabilidad última permanece en el responsable[643].

En cuanto a los requisitos generales que informan la satisfacción de estos derechos, existen una serie de disposiciones que vinculan a las dos partes, responsable y encargado, máxime si este tiene la posibilidad de satisfacción directa de los mismos. Desde el punto de vista formal, cualquier comunicación consecuencia de los referidos derechos debe hacerse de manera concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. Nos encontramos ante conceptos indeterminados que, al estar incluidos en una norma jurídica, adquieren la condición de conceptos jurídicos indeterminados[644]. Estamos ante una

[641] INFORMATION COMMISSIONNER'S OFFICE (ICO). Data controllers and data processors: what the difference is and what the governance implications are. p. 18.
[642] INFORMATION COMMISSIONER (JERSEY) AND DATA PROTECTION COMMISSIONER (GUERNSEY). Cloud Computing A guide for data controllers. Ob. Cit.
[643] EUROPEAN DATA PROTECTION SUPERVISOR. Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe. Ob. Cit. p. 14.
[644] El mejor estudio a nuestro juicio sobre este tipo de conceptos, en SAINZ MORENO, F. Conceptos jurídicos indeterminados, interpretación y discrecionalidad administrativa. Civitas, Madrid. 1976. 364 p. El autor recuerda que "la teoría de los conceptos jurídicos indeterminados no opone éstos a los determinados, sino que su sentido es dar una respuesta al problema que plantea la indeterminación de los conceptos".

proyección más del principio de transparencia al que ya se ha hecho mención en otro apartado de este trabajo y que ya hemos visto que por ejemplo en el derecho a la información se articula a través de la citada información por capas.

También en el plano formal el segundo inciso del art. 12.1 RGPD señala una doble vía para facilitar la información: verbalmente o por escrito. Para la primera es necesario que lo solicite el interesado y exigirá de poderse verificar la identidad por otros medios. En el caso de la segunda, se destaca en particular la vía electrónica. La cuestión que se suscita en este caso es si esa alternativa es susceptible de ser aplicada a todos los derechos o si del texto del artículo se pudiera derivar que solamente es en lo concerniente al derecho a la información. Cabría deducir esto segundo si se tiene en cuenta, por ejemplo, que el derecho de acceso al que antes nos hemos referido, se ha de satisfacer por escrito en su vertiente de copia de los datos. Cabe por tanto señalar que la opción es factible como regla general, sin perjuicio de su concreción en cada caso concreto.

En lo temporal, todos los derechos gozan de una homogeneidad en el plazo. Así, el responsable –o el encargado actuando en nombre del responsable– deberán comunicarlo en un mes a partir de la solicitud, susceptible de prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes y debiendo indicar en todo caso los motivos de la dilación. En caso de no cumplir el plazo de un mes, existe la necesidad de comunicar, sin dilación, las razones, así como las vías de recurso (art. 12.4 RGPD). Cabe subrayar que en el caso concreto del derecho de información, existen unas previsiones específicas por cuanto en el caso de que los datos se hayan recogido del interesado, será necesario que se satisfaga dicha obligación en el momento de recopilar los datos (art. 13.1), mientras que si no se obtienen del interesado, se ha de facilitar en el plazo máximo de un mes, o bien en la primera comunicación con el interesado, o bien cuando los datos se vayan a comunicar a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez (art. 14.3 RGPD).

En lo que concierne al coste, el RGPD es claro en cuanto a que la información facilitada o cualquier actuación en virtud de los referidos derechos será gratuita, aunque introduce la posibilidad de que el responsable cobre un canon razonable en función de los costes o incluso negarse a actuar cuando considere que se trate de solicitudes manifiestamente infundadas o excesivas. El uso de estos términos tan indeterminados (infundado o excesivo)

ha merecido algunas críticas[645], máxime cuando en la normativa actual se trata de un elemento parametrizado por cuanto hoy día por ejemplo el derecho de acceso se puede denegar cuando no hayan transcurrido doce meses desde la solicitud anterior (art. 30.1 ROPD). Es de esperar que este aspecto se concrete en pro de la seguridad jurídica y del quehacer diario de responsable y encargado, aunque en el caso de este último, parece razonable que el contrato incluya una consulta al responsable. En todo caso, la carga de la prueba, en una suerte de *in dubio pro interesado*, va a recaer siempre sobre el responsable del tratamiento.

En cuanto al ejercicio material de los derechos, son de naturaleza personalísima, de tal manera que es el titular de los datos quien deberá ejercerlos, o bien a través de su representante debidamente acreditado (art. 23 ROPD). Buena prueba de lo dicho es la previsión del art. 12.6 RGPD que recoge que cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud, podrá solicitar que se facilite la información adicional necesaria para confirmar su identidad. En este sentido, y dada la responsabilidad última del cliente, parece lógico que el proveedor pudiera requerir la colaboración de este a los efectos de llevar a cabo dicha identificación cuando le corresponda la satisfacción directa de los derechos. En la misma línea, el art. 11 RGPD contempla los tratamientos que no requieren de identificación y se dice que no se aplicarán los derechos de acceso, rectificación, supresión, limitación o el derecho a la portabilidad, excepto cuando el interesado, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación. En estos casos en los que de nuevo estamos ante un presupuesto ontológico del tratamiento, parece necesaria la comunicación entre proveedor y cliente con la finalidad de que en caso de que se ejercite ante el encargado del tratamiento, este ponga en conocimiento del responsable la identidad del interesado. Como se observa, la identidad de quien ejercer el derecho es una cuestión clave, y más en el caso de la nube. A título de ejemplo, el art. 7.3 de la normativa británica señala que cuando el responsable exige razonablemente mayor información de cara a identificar a la persona que ejerce el derecho, no está obligado a cumplir con el requerimiento de acceso a menos que se la haya satisfecho dicha información[646].

---

[645] DATA PRIVACY INSTITUTE-ISMS FORUM SPAIN. Estudio de impacto y comparativa con la normativa española de la propuesta de Reglamento General de Protección de Datos de la Unión Europea. 2016. Disponible en web: https://www.ismsforum.es/ficheros/descargas/estudio-reglamento-ue-dpi1353525776.pdf

[646] Art. 7.3 *Data Protection Act* (1998). http://www.legislation.gov.uk/ukpga/1998/29/section/7

Por continuar con el plano material, cualquiera de los anteriores derechos puede verse limitado por las causas señaladas en el art. 23 RGPD:

que se justifique en

- la seguridad del Estado;
- la defensa;
- la seguridad pública;
- la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales,
- otros objetivos importantes de interés público general de la UE o de EEMM
- La protección de la independencia judicial y de los procedimientos judiciales;
- la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;
- una función de supervisión, inspección o reglamentación vinculada
- la protección del interesado o de los derechos y libertades de otros;
- la ejecución de demandas civiles.

Fuente: elaboración propia

Y en todo caso con la concurrencia de un triple requisito: la medida legislativa será necesario que respete la esencia de los derechos y libertades fundamentales; será proporcionada y necesaria, y además incluirá una serie de disposiciones específicas (art. 23.2 RGPD): la finalidad del tratamiento, las categorías de datos; el alcance de las limitaciones establecidas; las garantías para evitar accesos o transferencias ilícitos o abusivos; la determinación del responsable o de categorías de responsables; los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza alcance y objetivos del tratamiento o las categorías de tratamiento; los riesgos para los derechos y libertades de los interesados, y el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta.

En el caso de estas limitaciones que vendrán establecidas por la normativa aplicable al responsable, puede tener trascendencia en la satisfacción de los derechos, particularmente cuando estos puedan ser ejercidos directamente ante el encargado, es decir, ante el

proveedor. En este sentido, caben dos opciones con la finalidad de salvaguardar el cumplimiento y teniendo en cuenta la responsabilidad última del responsable: o bien se recoge en el contenido del contrato la normativa aplicable y los casos en los que pueda existir una limitación, o bien como consecuencia de la necesaria notificación por parte del proveedor a su cliente. Es por ello que será necesario una comunicación fehaciente, a poder ser en el propio contrato con una descripción de los supuestos aplicables, o bien en el momento en el que se ejercite alguno de los derechos y sea obligada la notificación al responsable. Este deberá responder de manera inmediata satisfaciendo el derecho.

5 Portabilidad y cláusulas de salida

5.1 Interoperabilidad, estandarización y neutralidad como presupuestos necesarios

Se puede afirmar que el derecho a la portabilidad está pensado sobre todo para servicios de cloud computing[647], por lo que ver si el régimen jurídico que se ha configurado en el RGDP se ajusta a las características de esta tecnología –más allá de contribuir también al objetivo último de este trabajo– justifica su análisis en un apartado específico.

Tal es la importancia de la materia que vamos a tratar en este apartado, que incluso uno de los padres fundadores de Internet, Vinton Cerf, reclamaba en el conocido como *Open Cloud Manifesto* la necesidad de unos ciertos estándares que permitan la interoperabilidad y la portabilidad de los datos[648]. También el padre de la *World Wide Web*, Tim Berners-Lee, en su intervención de apertura en el *Mobile Internet World* en Boston en 2007, que llevaba el sugerente título "*Escaping the Walled Garden: Growing the Mobile Web with Open Standards*"[649], afirmaba que "la Web es una plataforma abierta en la que tú puedes construir otras cosas. Así es como consigues la innovación. La Web es universal: puedes utilizarla en cualquier hardaware, en cualquier sistema operativo, puede ser utilizada por gente de diferentes idiomas…es un campo en el que la gente puede ejercitar su creatividad". En fin, el Foro Económico Mundial de 2011 subrayó la importancia de hacer la portabilidad de los

[647]GONZÁLEZ-CALERO MANZANARES, F.R. Primera aproximación al Reglamento General de Protección de Datos. *Elderecho.com*. 28 de enero de 2016. Disponible en web: http://tecnologia.elderecho.com/tecnologia/privacidad/Aproximacion-Reglamento-General-Proteccion-Datos-dia-europeo-proteccion-datos_11_912055001.html

[648] FUNDACIÓN DE LA INNOVACION BANKINTER. Cloud Computing, la Tercera Ola de las Tecnologías de la Información. Ob. cit. p. 53.

[649] Acceso al texto completo de la intervención en el siguiente enlace: https://www.w3.org/2007/Talks/1114-tbl/text.html

datos más rápida, fácil y barata y facilitar la interoperabilidad para acelerar la adopción de la nube y el desarrollo de un mercado competitivo[650]. Sin embargo, como señalaba más recientemente la industria británica, los estándares que se necesitan para que se puedan mover las infraestructuras y aplicaciones entre proveedores cloud están todavía en una etapa temprana de desarrollo e implantación[651]. En nuestra doctrina, García Mexía, citando a Tim Berners-Lee, recuerda que algunas de las grandes empresas de Internet estarían generando "silos" inconexos y estancos de información, que ni los consumidores ni las empresas pueden muchas veces portar consigo de unas a otras[652]. En realidad, estamos ante un problema que no es nuevo y que ha sido consustancial al devenir de Internet y, lo que es más importante, su superación ha permitido que Internet se haya desarrollado como lo que hoy es. Como bien señala Renda, "la necesidad de asegurar una interoperabilidad fluida entre las nubes públicas está íntimamente relacionada con la necesidad de estándares abiertos que hagan posible la "federación de nubes" o *intercloud* en los próximos años, replicando el paradigma de la "red de redes" que ha hecho Internet posible"[653]. Estamos en realidad trasladando el fundamental debate de la neutralidad en la Red al fenómeno de la computación en nube. De ahí que no falten voces que hayan hablado ya de la *Cloud Neutrality*[654], debate para el que contamos con la suerte de tener todo el bagaje de las lecciones aprendidas de la neutralidad en la Red, sin perjuicio de que existen algunas diferencias relevantes: en particular la ausencia de una "moneda" común efectiva y la dificultad de auditar la utilización de recursos[655]. Previamente a desarrollar esta importancia y el tratamiento normativo y doctrinal que se le ha dado, debemos sin embargo marcar la distinción entre los referidos conceptos,

---

[650] WORLD ECONOMIC FORUM IN PARTNERSHIP WITH ACCENTURE. Advancing Cloud Computing: What to Do *Now?* 2011. Disponible en web: http://www3.weforum.org/docs/WEF_IT_AdvancedCloudComputing_Report_2011.pdf

[651] TECH UK. TechUK Cloud 2020 Vision. Keeping the UK at the forefront of cloud adoption", marzo de 2016. p. 3.

[652] GARCÍA MEXÍA, P. Internet y derecho en la era del cloud computing. *Blog La Ley en la Red*. 10 de febrero de 2014. Disponible en web: http://abcblogs.abc.es/ley-red/public/post/internet-y-derecho-en-la-era-del-cloud-computing-15823.asp/

[653] RENDA, A. Competition, Neutrality and Diversity in the Cloud. *Digiworld Economic Journal.* 2012. nº 85. p. 23. Disponible en web: ftp://ftp.repec.org/opt/ReDIF/RePEc/idt/journl/CS8501/CS85_RENDA.pdf

[654] GARCÍA MEXÍA, P. Cloud Computing. Sus dilemas legales. *Universidad Politécnica de Madrid*. Disponible en web: http://www.upm.es/sfs/Rectorado/Gabinete%20del%20Rector/Notas%20de%20Prensa/2010/2010-06/documentos/Derecho%20y%20Nube.pdf

[655] KESIDIS, G., URGAONKAR, B., NASIRIANI, N. y WANG, C. Neutrality in Future Public Clouds: Implications and Challenges. *8th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 16),* USENIX Association. Denver, Colorado. 2016. Disponible en web: https://www.usenix.org/system/files/conference/hotcloud16/hotcloud16_kesidis.pdf

teniendo en cuenta que la interoperabilidad y la portabilidad son conceptos que están interrelacionados entre sí, ya que sin interoperabilidad no hay portabilidad[656].

De acuerdo con la Organización Internacional de Normalización se puede definir la interoperabilidad como la posibilidad de que dos o más sistemas o aplicaciones puedan intercambiar información y utilizar mutuamente la información que ha sido intercambiada. En el caso concreto del *cloud*¸ el *Cloud Consumer Council* añade que la interoperabilidad debería verse como la capacidad de las nubes públicas, las nubes privadas y otros sistemas diversos en la compañía, para entender las interfaces de servicio y aplicaciones de otros de cara a cooperar e interoperar con cada uno[657]. Descendiendo a un mayor detalle, Gleeson y Walden señalan que en el caso de IaaS y de PaaS la interoperabilidad se refiere a las interfaces o APIs necesarias para que las interfaces de gestión de plataformas de virtualización operen entre diferentes proveedores; mientras que en el caso de SaaS la interoperabilidad es más sobre la compatibilidad de los formatos de datos, archivos de datos y protocolos[658].

Por su parte la portabilidad, parafraseando al RGPD que lo reconoce por primera vez como derecho, tal y como veremos luego con detalle, se puede definir como el derecho a recibir la información que se haya facilitado a un tercero en un formato estructurado, de uso común y lectura mecánico y transmitirlo a otro sin que lo impida el primero. En el entorno cloud, la Agencia Española de Protección de Datos, en su ya tratada guía sobre cloud computing, señalaba que las soluciones que ofrecen los proveedores de *cloud computing* pueden clasificarse como abiertas a la portabilidad o cerradas a la misma. Se podrá considerar una solución abierta a la portabilidad cuanto mayor sea la facilidad de un usuario para transferir todos sus datos y aplicaciones desde un proveedor de *cloud* a otro (o a los sistemas propiedad del cliente), garantizando la disponibilidad de los datos y la continuidad del servicio[659].

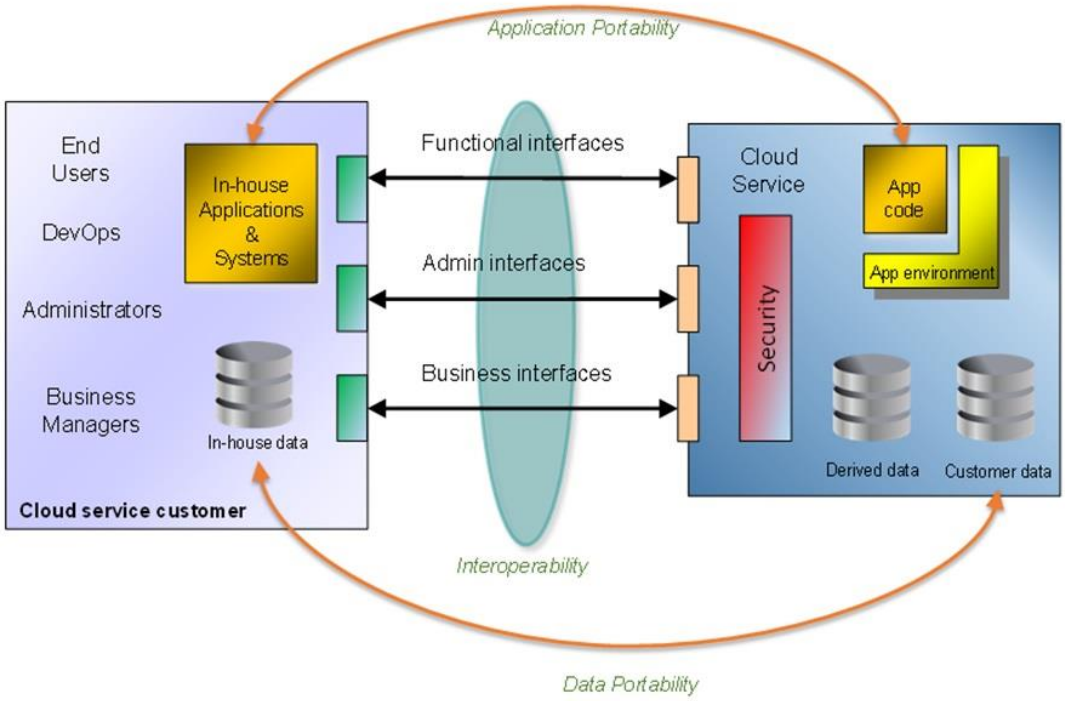
---

[656] MAQUEO RAMÍREZ, M.S., MORENO GONZÁLEZ, J. y RECIO GAYO, M. Lineamientos de Protección de Datos en el Cómputo en la Nube: Parámetros para su elaboración. *Centro de Investigación y Docencia Económicas*. México, septiembre de 2014. Disponible en web: https://cidecyd.files.wordpress.com/2014/09/white-paper-lineamientos-proteccion-datos-computo-nube-mx-18-sept-14-def.pdf

[657] CLOUD STANDARDS CONSUMER COUNCIL. Interoperability and Portability for Cloud Computing: A Guide", noviembre de 2014. Disponible en web: http://www.cloud-council.org/deliverables/CSCC-Interoperability-and-Portability-for-Cloud-Computing-A-Guide.pdf

[658] GLEESON, N.C. y WALDEN, I. It's a jungle out there'?: Cloud computing, standards and the law. *European Journal of Law and Technology*. Nov. 2014. Vol. 5. nº 2.

[659] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía para clientes que contraten servicios de Computing. Ob. cit. p. 8.



Elements of Interoperability and Portability for Cloud Services

Fuente: *European Committee for Interoperable Systems*[660]

En realidad, continuando con lo que hemos apuntado más arriba, interoperabilidad y portabilidad no dejan de ser respuestas a la conocida teoría de los denominados "jardines vallados" o de la "encerrona tecnológica"[661] que da lugar a la existencia de clientes cautivos[662]. Son muchos los motivos que han llevado a los grandes proveedores a impulsar

[660] EUROPEAN COMMITTEE FOR INTEROPERABLE SYSTEMS. Cloud Switching and the free flow of data – portability and interoperability of software and data across cloud services. 27 de junio de 2016. Disponible en web: http://www.ecis.eu/2016/06/special-paper-on-cloud-computing-portability-and-interoperability/

[661] En su informe, la Fundación Bankinter define *Technological lock-in* como un término que se utiliza para describir situaciones en las que existe una falta de compatibilidad entre las tecnologías de distintos proveedores, lo cual obliga a que un cliente que hace uso de las tecnologías de un determinado proveedor incurra en importantes costes de cambio para poder utilizar la tecnología de otro proveedor. De esta forma, el cliente está encadenado a la tecnología de su proveedor y estos elevados costes de cambio sirven de factor disuasorio ante el cambio. FUNDACIÓN DE LA INNOVACIÓN BANKINTER. Cloud Computing, la Tercera Ola de las Tecnologías de la Información. p. 123

[662] *Idem*. p. 51.

la supuesta encerrona[663]. En el ámbito específico del cloud esta pugna adquiere una particular relevancia por cuanto el salto a la nube supone poner todo el servicio computacional de cualquier compañía en manos de un tercero[664].

Precisamente por ello existe una corriente destinada a garantizar esa interoperabilidad, corriente a la que se han sumado las instituciones oficiales; y prueba de ello es cómo la Comisión Europea, en su documento "*Unleashing the potential of Cloud Computing"* señalaba como la primera de sus acciones la de reducir la "jungla de estándares". Esta corriente ha culminado en el reconocimiento del derecho a la portabilidad de los datos en el nuevo RGPD, aunque este está basado, como veremos, en un derecho reconocido a los interesados y no tanto en el esquema B2B que estamos tratando. Lo cierto es que esta diferenciación se puede llegar a afirmar que la ha demandado el propio mercado. Prueba de ello es que en el marco de la consulta pública evacuada por la Comisión Europea sobre el cloud computing y los datos donde algunas empresas y asociaciones de empresas enfatizaron que la portabilidad y la portabilidad no debería ser una obligación general o vinculante para todos los proveedores sino un elemento diferenciador competitivo que podría reducir o revisar las disfunciones competitivas y señalaron que en su opinión la interoperabilidad debería permanecer como una decisión propia de negocio[665].

Desde la perspectiva de las autoridades de protección de datos, la Agencia, en la referida Guía, afirma que la portabilidad debe tenerse en cuenta a la hora de utilizar servicios de cloud, sobre todo públicos, pues cuanto más cerrado a la portabilidad sea el proveedor mayor será la dificultad, o incluso imposibilidad, de poder realizar esa transferencia a un coste razonable que haga que, de facto, el cliente esté cautivo del proveedor[666]. El Grupo de Trabajo del artículo 29, en su Dictamen 05/2012 afirmaba, en referencia a la portabilidad, que actualmente (en 2012) la mayoría de los proveedores no hacen uso de formatos de datos estandarizados ni de interfaces de servicio que faciliten la interoperabilidad y la portabilidad

---

[663] EISEMANN, T.R., PARKER, G. y VAN ALSTYNE, M. Opening Platforms: How, When and Why? *Harvard Business Review*. 31 de agosto de 2008.

[664] CASCIOTTI VIGNOLO, S. y NAHABETIÁN BRUNET, L. Cloud Computing & Walled Gardens. *Revista de Derecho de la Universidad de Montevideo*. 2012. nº 21. p 23 y siguientes. Para más información sobre esta materia, ver también CHANG, V., WALTERS, R.J. y WILLS, G. Delivery and Adoption of Cloud Computing Services in Contemporary Organizations*. IGI Global*. Estados Unidos. 2015. 483 p.

[665] EUROPEAN COMMISSION. Synopsis report on the contributions to the public consultation on the regulatory environment for data and cloud computing. 12 de mayo de 2016. Disponible en web: https://ec.europa.eu/digital-single-market/en/news/synopsis-report-contributions-public-consultation-regulatory-environment-data-and-cloud

[666] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía para clientes que contraten servicios de Computing. p. 9.

entre diferentes proveedores[667]. La CNIL en Francia recuerda la importancia de que en el contrato se recoja una cláusula de reversibilidad/portabilidad señalando que se debe garantizar la fácil reversibilidad y portabilidad de los datos en un formato estructurado y ampliamente utilizado, a requerimiento del cliente y en cualquier momento[668]. Cabe aclarar que la referencia a la reversibilidad no es sino el ejercicio de la portabilidad teniendo como destinatario los sistemas del propio cliente. A nivel oficial, y con una proyección que va más allá de la portabilidad, también la Comisión Europea, tras recordar que entre 2013 y 2020 se doblará el porcentaje de datos almacenado en la nube [669], ha lanzado la iniciativa concerniente a la libre circulación de los datos, que en estos momentos se encuentra en fase de elaboración y que tiene uno de sus pilares fundamentales, vinculado a la interoperabilidad y a la estandarización, esa libre circulación entre los proveedores de servicios en nube.

Ahora bien, como señala la industria británica, el éxito dependerá de la voluntad y apertura de los decisores públicos en cuanto a conectar con la industria y sacar partido de su experiencia de cara a los detalles se necesitan[670]. Efectivamente, la industria, principal protagonista, se ha posicionado en numerosas ocasiones, al menos en los documentos públicos, en la necesidad de articular la interoperabilidad y garantizar consiguientemente la portabilidad. Esta paradoja entre asegurar el negocio y garantizar unos estándares ha sido puesta de manifiesto a ambos lados del Atlántico. Así, el NIST señalaba ya en 2009 que hay que definir unos estándares mínimos que permitan una integración de la nube, la portabilidad de las aplicaciones y de los datos; a la vez que evitar un exceso grado de detalle que impediría la innovación[671]. En nuestro caso, era la Comisión Europea en el documento de 2012 anteriormente citado, quien señalaba que "actualmente [en 2012] los vendedores individuales tienen un incentivo para luchar por el dominio "encerrando" a sus clientes, impidiendo acercamiento estandarizados y ampliamente reconocidos por la industria. A pesar de numerosos esfuerzos de estandarización, la mayoría impulsados por proveedores, las nubes pueden desarrollarse de una manera que olvida la interoperabilidad, la portabilidad

[667] ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 05/2012 on Cloud Computing. Ob. cit. p. 16.
[668] CNIL. Recommendations for companies planning to use Cloud computing services. ob. Cit. p. 10.
[669] COVASSI, B. DSM Free Flow of Data Initiative and emerging issues of data ownership, access and usability. 5 de noviembre de 2015. Disponible en web: https://ec.europa.eu/digital-single-market/en/news/digital-single-market-free-flow-data-initiative
[670] TECH UK. techUK Cloud 2020 Vision. Keeping the UK at the forefront of cloud adoption. Ob. Cit. p. 6.
[671] MELL, P. y GRANCE, T. Effectively and Securely Using the Cloud Computing Paradigm. *NIST, Information Technology Laboratory*. 2009. Disponible en web: http://csrc.nist.gov/organizations/fissea/2009-conference/presentations/fissea09-pmell-day3_cloud-computing.pdf

de los datos y la reversibilidad, todos ellos cruciales para impedir el encierro"[672]. En el citado *open cloud manifesto*[673] se recogen una serie de principios por parte de la industria que van enfocados a la consecución de ese objetivo: trabajar conjuntamente a través una colaboración abierta y un uso adecuado de los estándares en la consecución de retos como la interoperabilidad o la portabilidad; el no uso de las posiciones de mercado de un proveedor para hacer cautivos a los clientes; el uso de estándares aceptados cuando sea apropiado; cuando haya nuevos estándares o ajustes hay que ser juicioso y pragmático, asegurándose de que favorecen la innovación; cualquier esfuerzo debe estar basado en las necesidades del consumidor; y en definitiva hay que trabajar juntos. También la *Business Software Alliance (BSA)* llamaba a los proveedores de servicios en nube a trabajar conjuntamente para promover el desarrollo de estándares orientados al mercado y asegurar la interoperabilidad y la portabilidad en un proceso abierto y colaborativo[674]. Cuestión distinta es si, como ha apuntado algún autor, esta avalancha de iniciativas hace que estemos ante una verdadera jungla de estándares[675] y basta para ello observar, aunque ya con una cierta antigüedad, el informe elaborado por el Instituto Europeo de Estándares de Telecomunicaciones (ETSI) sobre la coordinación de los estándares cloud que concluyó sin embargo afirmando que el campo de los estándares es complejo, pero no es caótico y de ningún modo una "jungla"[676]. Esta última postura puede tener una cierta lógica si se tiene en cuenta que, con independencia del reconocimiento del derecho a la portabilidad como mandato jurídico en el RGPD, la realidad es que la portabilidad es posible hoy día por vía jurídica y por vía tecnológica. Bien es cierto que en el primero de los casos será necesario que se haya incluido en el contrato propiamente dicho, convirtiéndose así en obligación jurídica; mientras que en el segundo supuesto lo que nos encontraremos es ante un proceso más farragoso y complejo, y probablemente acompañado de un mayor coste, pero no de una imposibilidad en sí misma. No estaremos sin duda ante un derecho a la portabilidad en el sentido del RGPD, pero sí ante una portabilidad materialmente hablando. La Comisión Europea viene a confirmar esta realidad, como luego veremos, al afirmar que uno de los objetivos del RGPD

[672] EUROPEAN COMMISSION. Unleashing the potential of Cloud Computing. ob. Cit. p. 10.
[673] OPEN CLOUD MANIFESTO. A call to action for the worldwide cloud community. 2009. p. 5 y 6. Disponible en web: https://gevaperry.typepad.com/Open%20Cloud%20Manifesto%20v1.0.9.pdf
[674] BUSINESS SOFTWARE ALLIANCE. Cloud Computing Policy Agenda for Europe. Disponible en web: http://www.bsa.org/country/~/media/files/policy/engb/bsaeucloudagenda.ashx
[675] GLEESON, N.C. y WALDEN, I. It's a jungle out there'? Cloud computing, standards and the law. Ob. Cit.
[676] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. Cloud Standards Coordination Final Report. noviembre de 2013. Disponible en web: http://www.etsi.org/images/files/events/2013/2013_csc_delivery_Ws/csc-Final_report-013-csc_Final_report_v1_0_pdF_format-.pdF

es poder transferir los datos de un proveedor a otro con "mayor facilidad"[677]. No se habla por tanto de hacer frente a una imposibilidad de transferencia, sino a una herramienta subjetiva que la facilita. Recientemente ha confirmado esta misma postura el Grupo de Trabajo del artículo 19 al afirmar que el primer objetivo de la portabilidad de los datos es facilitar el cambio de un proveedor de servicios a otro y recordar a su vez que a pesar de que la portabilidad es un nuevo derecho, otros tipos de portabilidad ya existían o están siendo debatidas en otras áreas normativas (por ejemplo en el contexto de una finalización de contrato, el *roaming* en los servicios de comunicaciones o el acceso transfronterizo a los servicios)[678].

En el plano doctrinal, y más allá de la preocupación manifestada al comienzo de este apartado, Gastón Fourcade describe gráficamente que cuando hablamos de portabilidad nos referimos a la capacidad de cambiar de entorno luego de implementar un modelo cloud: la posibilidad de cambiar de proveedor, agregar nuevos proveedores cloud, pasar de un cloud público a uno privado, o comenzar a utilizar una nueva infraestructura que no sea cloud. Y añade que cuando un proveedor ofrece alta portabilidad, está asegurando al cliente flexibilidad, libertad y capacidad de decisión[679].

Si bien como ya se ha visto, la interoperabilidad y la portabilidad en los servicios TIC ha jugado un papel importante ya desde hace muchos años, es igualmente cierto que su reconocimiento normativo es bastante más reciente. En este sentido, al igual que muchos otros aspectos que luego han recibido desarrollo normativo, la primera perspectiva desde la que se trató fue la de la competencia. Siguiendo a De Filippi y Belli[680], podemos recordar cómo en la UE la interoperabilidad surgió como un elemento de competencia en el sector TIC ya en los años 80 en el caso IBM, tendencia que fue reiterada en 2004 por el tribunal de primera instancia cuando confirmó una decisión de infracción contra Microsoft por no facilitar información de interoperabilidad a su competidor[681]. A mayor abundamiento, cuando la

[677] COMISIÓN EUROPEA. Comunicado de Prensa. La Comisión propone una reforma general de las normas de protección de datos para aumentar el control de los usuarios sobre sus propios datos y reducir los costes para las empresas. 25 de enero de 2012. Disponible en web: http://europa.eu/rapid/press-release_IP-12-46_es.htm

[678] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on the right to data portability. 13 de diciembre de 2016. Disponible en web: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf

[679] FOURCADE, G. Seis variables para analizar antes de saltar a la nube. *IBM.* 2011. Disponible en web: http://www.ibm.com/ar/services/pdf/final_seis_variables_para_analizar_antes_de_saltar_a_la_nube.pdf

[680] DE FILIPPI, P. y BELLI, L. Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation. *European Journal of Law and Technology.* 2012. Vol. 3. nº 2.

[681] Unión Europea. Tribunal de Primera Instancia (Gran Sala). Caso Microsoft Corp (T-201/04). Sentencia de 17 de septiembre de 2007. Disponible en web: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d536ba3e5909904dc6ad82d573

Comisión Europea presentó su propuesta de Reglamento de Protección de Datos en enero de 2012, subrayaba como uno de los cambios esenciales el tener un acceso más fácil a sus propios datos y poder transferir sus datos personales de un proveedor de servicios a otro con mayor facilidad (el derecho a la «portabilidad de los datos»), lo que aumentará -y aquí la perspectiva señalada- la competencia entre servicios[682]. Más recientemente Graef[683] recordaba en el campo de las redes sociales cómo la portabilidad y la interoperabilidad se pueden afrontar desde la perspectiva del Derecho de la Competencia comunitario. Un ejemplo muy práctico lo tenemos recientemente en la resolución de la Comisión Europea respecto a la adquisición de WhatsApp por Facebook en la que el elemento de la portabilidad fue objeto expreso de análisis[684].

5.2 El derecho a la portabilidad como derecho de los interesados

Sin embargo, a pesar de estas contundentes preocupaciones, la portabilidad de los datos sea en entornos cloud o sea en cualquier otro tipo de entorno tecnológico, no había sido recogida hasta muy recientemente, si bien esta contundencia, como vamos a ver, es respecto a su consideración como derecho subjetivo de los interesados. En la actual normativa no viene exigida. Solamente se contempla, -bien en textos normativos o a través de acciones de la comisión[685]- como un requisito para los sistemas de tratamiento automático de datos para cooperar sin problemas. Es por ello que ha tenido suma importancia la introducción del derecho a la portabilidad de los datos en el artículo 20 del RGPD. Se trata de un derecho que ha sufrido en cierta medida vaivenes durante la tramitación, por cuanto fue introducido en la propuesta de la Comisión Europea en enero de 2012, se eliminó en la fase del Parlamento Europeo en 2014, se volvió a introducir en la versión aprobada por el Consejo en 2015 y finalmente se ha introducido en el texto definitivamente aprobado. Desde el punto de vista de su naturaleza se viene afirmando que se trata de un derecho que refuerza el

dedc7a69.e34KaxiLc3qMb40Rch0SaxyKaxr0?text=&docid=62940&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=20703

[682] COMISIÓN EUROPEA. Comunicado de Prensa. La Comisión propone una reforma general de las normas de protección de datos para aumentar el control de los usuarios sobre sus propios datos y reducir los costes para las empresas. Ob. cit.

[683] GRAEF, I. Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union. *Telecommunications Policy 2015*. Vol. 39, No. 6. p. 502-514. Disponible en web: http://dx.doi.org/10.2139/ssrn.2296906

[684] En concreto en el apartado 113 de la Resolución del expediente concreto. EUROPEAN COMMISSION. Case No COMP/M.7217 - FACEBOOK/ WHATSAPP. 3 de octubre de 2014. Disponible en web: http://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf

[685] SCHELLEKENS, B.J.A. The European Data Protection Reform in the light of cloud computing. *Tilburg University*. 2013. 79 p.

derecho de acceso a los propios datos, y más concretamente, en gráficas palabras de Ramón Miralles, estamos ante una prestación *Premium* del tradicional derecho de acceso[686], aunque como vamos a ver en el siguiente párrafo, a nuestro juicio esa afirmación es matizable, considerando que sí que tiene una sustantividad propia.

Desde el punto de vista de su contenido, se viene diciendo que el derecho a la portabilidad tiene una doble vertiente que comprende dos facultades: obtener una copia de sus datos personales en un formato electrónico estructurado y de uso habitual; y transferir sus datos, y otras informaciones que haya facilitado, de un sistema de tratamiento electrónico a otro[687]. Sin embargo, a nuestro juicio es más razonable la postura que parecía adoptarse en el documento inicial de la Comisión Europea en el que se puso de manifiesto que en realidad el contenido del derecho es uno: el derecho a transferir datos de un sistema de tratamiento electrónico a otro, sin que se lo impida el responsable del tratamiento; mientras que, a modo de condición previa y con el fin de seguir mejorando el acceso de las personas físicas a sus datos personales, establece el derecho de obtener del responsable esos datos en un formato electrónico estructurado y de uso habitual. Es decir, esta segunda vertiente se puede ver como una facultad derivada del derecho de acceso, siendo el primero el contenido del derecho a la portabilidad propiamente dicho. El Grupo de Trabajo del artículo 29, en sus Directrices sobre el derecho a la portabilidad vuelve a la doble vertiente en cuanto al contenido aunque no deja de mencionar que el derecho a recibir los datos personales complementa el derecho de acceso[688].

El texto que finalmente ha recogido el derecho a la portabilidad lo contempla con determinadas condiciones cuales son (art. 20 RGPD): que solamente debe aplicarse cuando el interesado haya facilitado los datos personales dando su consentimiento o cuando el tratamiento sea necesario para la ejecución de un contrato; que no debe ejercerse en contra de responsables que traten datos en el ejercicio de sus funciones públicas; que no debe obligar al responsable a adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles; y que el ejercicio de este derecho no puede afectar a los derechos y libertades

[686] MIRALLES, R. El derecho a la portabilidad de los datos personales o prestaciones "premium" del tradicional derecho de acceso; en VALERO TORRIJOS, J. La protección de datos personales en internet ante la innovación tecnológica riesgos, amenazas y respuestas desde la perspectiva jurídica. Aranzadi. 2013. p. 273 a 290.

[687] MIRALLES R., El derecho a la portabilidad de los datos personales. *Abogacía.* 15 de noviembre de 2012. Disponible en web: http://www.abogacia.es/2012/11/15/el-derecho-de-la-portabilidad-de-los-datos-personales/

[688] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on the right to data portability. p. 4.

de otros. A ello se añade que ha de tratarse de datos “que le incumban” y que sea él el que los haya “facilitado” al responsable. Estos dos aspectos han sido desarrollados por el Grupo de Trabajo del artículo 29 que básicamente ha señalado que lo primero conlleva que los datos anónimos o los que no a afectan al interesado no caerían dentro del ámbito de aplicación de este derecho (aunque sí los pseudónimos); y lo segundo incluiría los datos referidos a la actividad del interesado resultante de la observancia de su comportamiento pero no un análisis subsiguiente de dicho comportamiento, que quedarían fuera del derecho a la portabilidad de los datos[689].

Resulta muy importante por tanto matizar que, al igual que en el resto de derechos, el derecho que configura aquí el RGPD no es un derecho que le corresponda al responsable o cliente del prestador de servicios en nube, que es el supuesto que venimos manejando en este trabajo. No estamos hablando de un derecho susceptible de ser aplicado en el marco de las relaciones B2B, sino que se trata de un derecho, insistimos, tal y como está configurado, que le corresponde al interesado titular de los datos respecto al responsable de los mismos. Cuestión distinta es que, al igual que con el resto de derechos, sea inevitable que el encargado cumpla con los mismos parámetros que los establecidos para el responsable con la finalidad de que la portabilidad de los datos en ese entorno de nube en el que se está dando el tratamiento por cuenta de terceros, sea realmente efectivo. Cuestión distinta además será el hecho de que sea altamente recomendable recoger dentro de la relación contractual entre proveedor encargado y responsable cliente, la existencia de un derecho derivado del contrato suscrito. Recordemos a este respecto que con base en el artículo 28.3.e) RGPD el encargado, es decir el proveedor, tiene que asistir al cliente, a través de medidas técnicas, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto, entre otros, del derecho a la portabilidad. En definitiva, las exigencias de interoperabilidad que habilitan el ejercicio del derecho a la portabilidad, son perfectamente aplicables, jurídicamente, al prestador de servicios en nube.

En cuanto a la forma de ejercer este derecho, el RGPD (art. 20.2) ha contemplado que el interesado tiene derecho a que los datos personales se transmitan directamente de un responsable del tratamiento a otro, cuando sea técnicamente posible. A ello se añade el conjunto de elementos comunes a la totalidad de los derechos que corresponden al interesado y que afectan a su ejercicio por parte de este o a su satisfacción por parte del

[689] *Idem.* p. 9.

responsable, sin perjuicio de la mencionada, razonable e incluso obligatoria satisfacción por parte del encargado proveedor de los servicios en nube. De conformidad con el artículo 12 RGPD, el responsable deberá entregar los datos o trasladarlos a otro proveedor (reversibilidad o portabilidad) en el plazo de un mes desde la solicitud, plazo prorrogable por otros dos meses. Además, si decide no satisfacer ninguno de los dos derechos, el de obtención de la copia o el de la portabilidad, es el responsable, aquí sí, el que informará al interesado sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales. Desde el punto de vista económico el referido precepto contempla que el derecho a la portabilidad de los datos, al igual que el resto, tiene un carácter gratuito salvo que sean peticiones manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo. En este caso, el RGPD le da al responsable dos opciones, cuales son cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o realizar la actuación solicitada, o negarse a actuar respecto de la solicitud.

Esta última disposición requiere de una explicación en cuanto a las vertientes del derecho a la portabilidad que hemos tratado. Y es que, si bien es razonable el cobro de un canon tanto por parte del responsable como por parte del encargado proveedor de la nube, en lo que concierne a la negativa puede ser una opción no realizable. En las vertientes anteriormente tratadas la obtención de una copia en un formato electrónico estructurado y de uso habitual es una vertiente en la que se puede dar el referido abuso, y particularmente en su naturaleza repetitiva. Sin embargo, la portabilidad puede agotarse en algunas ocasiones, en muchas ocasiones, en un solo acto. Pensemos que dicha portabilidad se ejercer respecto a la totalidad de los datos ya sea en su modalidad de reversibilidad o de traslado de la información a terceros.

Hemos venido señalando que la portabilidad en cuanto que derecho subjetivo está planteado como derecho del interesado[690] y consiguientemente no está configurado como tal, como un derecho susceptible de ser ejercicio por el responsable de los datos respecto del encargado. Sin embargo, ya se ha venido señalando que, en el marco de las relaciones entre el cliente responsable y el proveedor encargado, aquel le puede pedir a este el ejercicio del referido

[690] Uno de los debates abiertos es que debería valorarse si el derecho a la portabilidad realmente debe ser una facultad vinculada a un derecho fundamental o nos encontramos ante un instrumento más vinculado al derecho de los consumidores o al derecho mercantil. MIRALLES R. El derecho a la portabilidad de los datos personales. Ob. cit.

derecho. Es necesario garantizar que el cliente, como responsable, al hacer uso de los servicios proporcionados por el proveedor del servicio, como encargado, pueda tener en todo momento acceso y/o posibilidad de recuperación de los datos personales que son tratados en la nube[691]. Hay que tener en cuenta que, a pesar de su repetida consideración como novedad en el RGPD, esto se encuentra ya contemplado en la normativa actual vinculado a las denominadas cláusulas de salida o a qué ocurre cuando se pone fin a la relación contractual entre el cliente y el proveedor de servicios en nube. La propia industria es consciente de la inclusión de este tipo de clausulado y en su propuesta de Código de Conducta a nivel europeo, apunta la necesidad de incluir la posibilidad de que el cliente haga una copia de los datos almacenados o que se transmitan los datos a otra infraestructura. Pero van más allá, subrayando la necesidad de incluir los formatos disponibles para la reversión y la descripción de los mecanismos para la devolución. Y añaden que el proveedor deberá borrar o hacer irrecuperables las copias, salvo que así lo pueda contemplar el contrato o una ley (por ejemplo, obligaciones de conservación referidas a impuestos, garantías…etc.).

Y es que, desde el punto de vista normativo, el artículo 12.3 LOPD ya contempla la cláusula de portabilidad en su vertiente de reversibilidad, ya que señala que una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. Por otra parte, la Agencia venía indicando que el deber de devolución al que se refiere el artículo 12.3 podría verificarse mediante la entrega directa de los datos al propio responsable del tratamiento o mediante la realización de dicha entrega al encargado del tratamiento que este designase, toda vez que en este segundo caso el encargado actuaría como mero mandatario del responsable, siendo precisamente éste el que establece a quién han de entregarse los datos en su nombre y por su cuenta[692]. Siguiendo esta doctrina, el ROPD recoge igualmente la reversibilidad, pero añade un verdadero supuesto de portabilidad al señalar que los datos podrán ser devueltos al encargado que el responsable hubiera designado, al igual que cualquier soporte o documento en el que conste cualquier dato objeto de tratamiento. En este caso sí que estaríamos ante una portabilidad exigible por el cliente-responsable al proveedor-encargado. E incluso cabría decir que esta portabilidad en el ROPD no está exclusivamente contemplada

[691] MAQUEO RAMÍREZ, M.S., MORENO GONZÁLEZ, J. y RECIO GAYO, M. ob. cit. p. 62.
[692] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Encargado del tratamiento y obligación de devolución de documentación. Informe 34/2006.

cuando se finaliza la relación contractual sino que como proyección de la misma, y al amparo de lo previsto en el párrafo segundo del artículo 20.3 ROPD[693], el proveedor, a indicación del cliente, podrá hacer llegar una copia de los datos a un tercero, que puede ser otro proveedor para la prestación de un servicio, sin incurrir en responsabilidad alguna.

5.3 Las cláusulas de salida

Pero volviendo a la finalización de la relación contractual, hay que tener en cuenta que se puede dar no solamente como consecuencia del cumplimiento por parte del proveedor, sino que, como apunta la Agencia, por otras circunstancias ajenas al contrato, como podría ser el fin de la prestación de algún tipo de servicio por parte del proveedor, el cambio de su política comercial o del marco regulatorio. Esta previsión no está expresamente contemplada en el RGPD por cuanto en las relaciones entre responsable y encargado se recoge que, a elección de aquel, este suprimirá o devolverá todos los datos una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros (artículo 28.3.g)).

Como ya hemos apuntado, dentro de estas relaciones entre el cliente y el proveedor, también se plantea qué ocurre con los datos una vez concluye la relación. Nos estamos refiriendo a las denominadas cláusulas de salida. Al respecto la Agencia Española de Protección de Datos señala que deben preverse mecanismos que garanticen el borrado seguro de los datos cuando lo solicite el cliente y, en todo caso, al finalizar el contrato[694]. Sin embargo, como se acaba de ver en el último inciso del artículo 28.3.g) RGPD el proveedor deberá conservar los datos cuando exista una norma que así lo obligue. Lo mismo se contempla en el ROPD y más concretamente en su artículo 22.2 que supone para el proveedor la necesidad de conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el cliente. Hay que observar en este sentido los matices

[693] El artículo 20.3 ROPD reza como sigue: "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 al que se refiere el apartado 2 del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.
No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo".

[694] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía para clientes que contraten servicios de Cloud Computing. ob. cit. p. 18.

diferenciadores. En realidad, con base en la redacción actual, el proveedor no puede conservar los datos por una obligación legal, sino que, con base en el párrafo segundo del artículo 22.1, no procede la destrucción de datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos al cliente, que es quien deberá garantizar la conservación. Así lo ha reiterado la Agencia, entre otros, en su informe 0472/2008 y de una manera más detallada el Informe 283/2004, que vino a recordar que de conformidad con el art. 1157 CC y con la jurisprudencia del TS, la prestación del servicio de tratamiento de datos se ha de considerar cumplida una vez ésta ha concluido, y a pesar de la devolución de la información, el encargado del tratamiento deberá poder conservar los datos objeto de la prestación mientras se pudieran derivar responsabilidades de su relación con el responsable del fi chero y procediendo al bloqueo de datos, para no poder utilizarlos durante ese tiempo.

En este punto resulta necesaria la distinción conceptual entre el bloqueo y la destrucción de los datos. Como señala el art. 5.1.b) ROPD el bloqueo "consiste en la identificación y reserva de los mismos [de los datos] 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.". Respecto a la forma de llevar a cabo dicho bloqueo, como señalara la Agencia en su informe de Agencia de 5 de junio de 2007 "deberá efectuarse de forma tal que no sea posible el acceso a los datos por parte del personal que tuviera habitualmente tal acceso, por ejemplo, el personal que preste sus servicios en el centro consultante, limitándose el acceso a una persona con la máxima responsabilidad y en virtud de la existencia de un requerimiento judicial o administrativo a tal efecto. De este modo, pese a permanecer el tratamiento de los datos, el acceso a los mismos quedaría enteramente restringido a las personas a las que se ha hecho referencia".

En el caso de la destrucción de los datos, se podría incluir dentro de un concepto más amplio al que recurre el NIST cual es el de *higienización* (sanitization) de los datos que define como un término general referido a las acciones adoptadas para convertir los datos en irrecuperables por medios ordinarios o extraordinarios. En el mismo se incluirían tres métodos: limpiar, purgar y destruir los datos, variando las herramientas y las técnicas en función del dispositivo que los almacene. La destrucción en concreto es definida como un método de higienización de los datos que convierte en inviable la recuperación de los datos

utilizando el estado del arte de las técnicas de laboratorio y que conlleva la imposibilidad subsiguiente de almacenar los datos[695].

Sentada esta distinción, en caso de que se proceda a la destrucción, y con base en las indicaciones de la Agencia, un mecanismo apropiado es requerir una certificación de la destrucción emitido por el proveedor de cloud computing o por un tercero[696]. Se trata de una cuestión no menor si se tienen en cuenta las sanciones a las que se podría enfrentar. Y es una cuestión que preocupa a las empresas que contratan servicios de este tipo por tres razones fundamentales: afecta a organizaciones incluyendo firmas de abogados que almacenan información privilegiada, proveedores de salud que almacenan informes médicos, universidades que almacenan expedientes, empleadores que almacenan datos de seguridad social…etc; las empresas prometen a sus clientes y a ellos mismos que van a destruir datos sensibles después de un periodo de tiempo determinado y muchas de estas promesas estás enumeradas en contratos vinculantes; y en tercer lugar, mientras dichos datos se encuentren en la nube, son susceptibles de verse atacados[697]. A ello se añaden las dificultades desde el punto de vista técnico, por cuanto los datos en papel pueden ser destruidos, los datos en un ordenador tradicional pueden ser sobreescritos, y el disco duro como tal puede ser destruido[698]. Y sin embargo, la destrucción de los datos almacenados por un proveedor en nube, como apuntan Henriques y Ding, es complicada por tres factores tecnológicos: persistencia de los datos, redundancias y respaldos[699]. También a nivel oficial la ENISA

[695] KISSEL, R., REGENSCHEID, A, SCHOLL, M. y STINE, K. Guidelines for Media Sanitization. *National Institute of Standards and Technology*. Diciembre de 2014. Disponible en web: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

[696] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía para clientes que contraten servicios de Cloud Computing. ob. cit. p. 18.

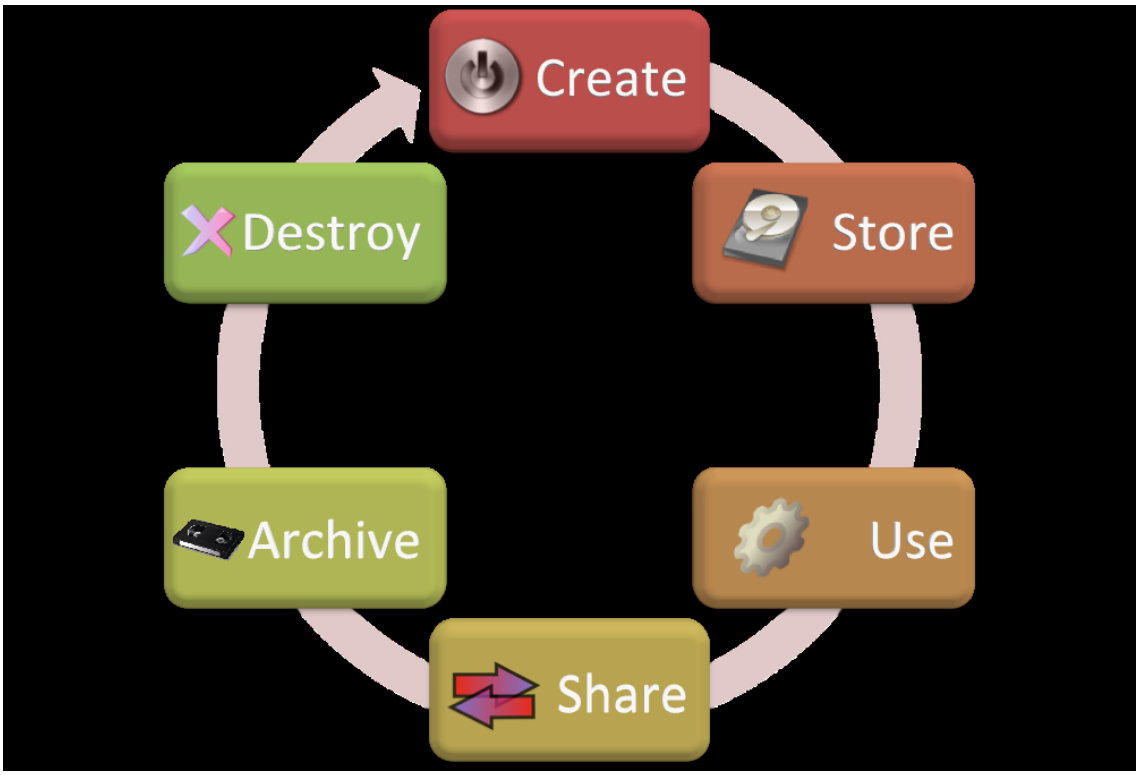
[697] HENRIQUES, M. y DIGN, J. Purging the Cloud: Data Destruction in the Age of Cloud Computing. *Womble Carlyle*. 23 de junio de 2014. Disponible en web: http://www.wcsr.com/resources/pdfs/henriquescloud0612.pdf

[698] Para una descripción de los mecanismos organizativos, técnicos y jurídicos, ver VELAZQUEZ YANEZ, H. Paso a paso: Destrucción de soportes y documentos conforme a la normativa de protección de datos personales. *www.legaltoday.com* 27 de febrero de 2016. Disponilbe en web: http://www.legaltoday.com/blogs/nuevas-tecnologias/blog-ecija-2-0/paso-a-paso-destruccion-de-soportes-y-documentos-conforme-a-la-normativa-de-proteccion-de-datos-personales De una manera más global o abstracta, INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS. Estudio sobre recomendaciones generales para la destrucción segura de datos personales en ambiente físico y electrónico. diciembre de 2014. Disponible en web: http://inicio.ifai.org.mx/DocumentosdeInteres/Estudio_sobre_destruccion_segura_DP.pdf

[699] HENRIQUES, M. y DIGN, J. Purging the Cloud: Data Destruction in the Age of Cloud Computing. ob. Cit. En la misma línea, STUTZMAN, K. Data Destruction – Protecting private data when moving to or from a cloud service. *Ongoing Operations.* 2012. Disponible en web: http://ongoingoperations.com/blog/2012/12/data-destruction-protecting-private-data-cloud-service/

señalaba como uno de los riesgos el borrado de datos inseguro o incompleto[700]. Hoy día borrar los datos ya no se puede conseguir simplemente apretando un botón[701].

En realidad estamos ante una proyección más de las medidas de seguridad a las que se ha hecho mención en el apartado anterior. Siguiendo a la *Cloud Security Alliance* se puede decir que sería la última fase del ciclo de vida de los datos[702]:



Fuente: *Cloud Security Alliance*

Es precisamente la propia CSA la que ha reconocido, en línea con lo apuntado más arriba, que la destrucción de los datos es extremadamente difícil en un entorno multiposesión y el proveedor de la nube debería utilizar un cifrado fuerte del almacenamiento que haga los datos ilegibles cuando el almacenamiento sea reciclado, enajenado, o accedido por cualquier

[700] ENISA. Cloud Computing Benefits, risks and recommendations for information security. Ob. Cit. p. 7.
[701] FINANCIAL TIMES. Cloud computing hinders data deletion. 18 de marzo de 2013. Disponible en web: https://www.ft.com/content/0e8aad72-7444-11e2-80a7-00144feabdc0
[702] CLOUD SECURITY ALLIANCE. Guía para la seguridad en áreas críticas de atención en *Cloud Computing*. Volumen 2. noviembre 2009. p. 21. Disponible en web: https://ccsk-es.cloudsecurityalliance.org/des88_GUIA_CSA_PARA_LA_SEGURIDAD_EN_AREAS_CRITICAS_DE_ATENCION_EN_CLOUD_COMPUTING_V2.pdf

medio distinto a las solicitudes, procesos o entidades autorizadas[703]. Y es que hay que tener en cuenta que, en el entorno actual de computación en nube, los centros de datos necesitan opciones seguras y económicas para reutilizar las configuraciones de sistemas de almacenamiento de la empresa sin tener que reconstruirlas[704].

La propia Agencia ha señalado que en caso de que se contrate un servicio de destrucción de documentos, resultará responsable del tratamiento la empresa o entidad que contrate dicho servicio, respondiendo la empresa prestadora del servicio en los términos de un encargado[705]. Con base en esta postura cabría decir que el prestador de servicios en nube podría certificar la destrucción de los datos, aunque la industria ha reconocido históricamente que la destrucción de datos puede ser muy difícil de demostrar para el proveedor. O bien podría recurrir a un tercero que sea designado por el cliente o bien que sea designado por el propio prestador de servicios en nube con el conocimiento del responsable. Estaríamos en este último caso ante una manifestación más de subcontratación, integrada como una más de las prestaciones del servicio, si bien en este caso sería para la culminación del mismo.

En definitiva y como se ha podido observar en este apartado, existe una clara concienciación normativa y de la industria por garantizar una interoperabilidad que permita la portabilidad. El hecho de que se haya configurado como un derecho subjetivo de todo interesado en el RGPD exigirá de la industria continuar en los esfuerzos en pro de la portabilidad. Ello favorecerá a su vez que en el seno de las relaciones B2B la portabilidad sea también una realidad, sin perjuicio de las exigencias normativas hoy ya existentes.

En cuanto a las vertientes de las cláusulas de salida, una vez más las certificaciones juegan un papel clave, máxime en una tecnología que está basada en un sistema de multiposesión, en un continuo dinamismo y en una cadena de subcontrataciones. Será esta la vía más adecuada para garantizar al responsable en primer lugar y a los interesados en último, que los datos no permanecen en manos del proveedor, más allá de lo que venga exigido por disposiciones normativas que, en todo caso, deberán estar limitadas, en pro del principio general de calidad de los datos, al tiempo estrictamente necesario para el cumplimiento de las mismas.

---

[703] *Idem.*
[704] BLANCO CERTIFIED DATA ERASURE. Soluciones de borrado de datos para centro de datos y seguridad de computación en nube. *Blanco White Paper.* 2ª edición. 26 de noviembre de 2013. P. 9, https://www.ontrackdatarecovery.es/CMS/PDF/white-paper-data-centre-es.pdf
[705] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Informe 0227/2010.

En conclusión, con base en lo desarrollado en este apartado, cabe considerar que el esquema de portabilidad en la nube en el seno de las relaciones B2B es perfectamente factible con base en el actual régimen jurídico, más allá de las exigencias tecnológicas. Se trata de una característica que forma parte de la libertad contractual, respondiendo en última instancia a la sana competitividad de los operadores tecnológicos.

"Cloud is about how you do computing, not where you do computing"

Paul Maritz,

VMware CEO

*"A cloud without robust data protection is not the sort of cloud we need***"**

25 de noviembre de 2010, Neelie Kroes

Vicepresidenta de la Comisión Europea para la Agenda Digital

CAPÍTULO IV: LOS ELEMENTOS OBJETIVOS DE LA PRIVACIDAD EN LA NUBE

1 Las transferencias internacionales y la subcontratación

1.1 Introducción

Si hay un tema fundamental en la prestación de servicios en nube, este suele ser el de las transferencias internacionales de datos y, particularmente, el de la subcontratación. A estas cuestiones vamos a dedicar los dos primeros apartados de este capítulo. Es tal su importancia en el seno de este trabajo, que si llegásemos a la conclusión de que el régimen jurídico actual no resulta válido para satisfacer estas dos características tan consustanciales a la nube, muchas de las reflexiones que se han llevado a cabo en páginas anteriores y que se realizarán con posterioridad, carecerían de sentido. En definitiva, la respuesta que se dé a este apartado afecta de una manera radical a la hipótesis global de este trabajo: si hace falta o no un régimen jurídico diferenciado y nuevo para la computación en nube.

Marzo Portera caracteriza el cloud computing como un modelo basado en la continua subcontratación de servicios y descentralización geográfica y transfronteriza de bases de datos que pueden almacenar información sobre individuos o personas físicas[706]. Por su parte, Ramón Miralles afirma que, entre los cuatro principales problemas de la relación entre protección de datos y cloud computing están las dificultades de encajar jurídicamente y con suficiente agilidad las situaciones de tratamiento de los datos por cuenta de terceros: el

[706] MARZO PORTERA, A.M. Privacidad y cloud computing, hacia dónde camina Europa. *Revista de Sociales y Jurídicas*. 2012. Vol. 1. nº 8. p. 202-229.

encargado del tratamiento cloud y las posibles subcontrataciones; y las problemáticas derivadas del movimiento internacional de datos[707].

En el plano normativo, la referida vinculación parece estar implícita en el RGPD y más concretamente en el último inciso del art. 45 que recoge el principio general de transferencias: "Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, *incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional*".

En lo que concierne a las autoridades de protección de datos, el Grupo de Trabajo del art. 29 ha recordado en su ya muchas veces citado Dictamen 05/2012, que "la computación en nube se basa a menudo en la total falta de ubicación estable de los datos en la red del proveedor. Los datos pueden encontrarse en un centro de datos a las 2 horas y en el otro lado del mundo a las 16 horas. Por tanto, el cliente rara vez se encuentra en posición de saber en cualquier momento en que lugar están situados, almacenados o transferidos los datos"[708]. En palabras de la Agencia Española de Protección de Datos: "Especialmente importante, dadas las características propias de los servicios de *cloud computing*, es establecer mecanismos para permitir que las subcontrataciones que se realicen en este contexto de transferencias internacionales se gestionen con fluidez, asegurando al mismo tiempo que el cliente responsable tiene información suficiente sobre los subcontratistas, o potenciales subcontratistas, y mantiene la capacidad de tomar decisiones"[709].

Desde el punto de vista doctrinal, los profesores Hon y Millard, recuerdan que "muchos proveedores de servicios cloud implican el uso de subproveedores de tal modo que la localización del centro de datos relevante será la de aquel centro de datos utilizado por el subproveedor en la capa más baja de "*cloud stack*"[710]. De hecho, apuntan los mismos

[707] MIRALLES, R. Cloud computing y protección de datos. *Revista de Internet, Derecho y Política*. 2010. nº 11. p. 14-23.
[708] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 5/2012 sobre computación en nube. ob. cit.
[709] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Orientaciones para prestadores de servicios de Cloud Computing. p.8. disponible en web: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/ORIENTACIONES_Cloud.pdf
[710] HON, K., MILLARD, C. y MILLARD, C. Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the Eea? The Cloud of Unknowing, Part 4. *SCRIPTed*. abril 2012. Vol 6. Issue 1. p. 25-

profesores, se puede decir que el cloud es "*data center-centric"*[711]. En palabras también de Cotino Hueso, "Casi por defecto, el uso de la nube implica el trasiego internacional de datos, bien porque el prestador de servicios esté en el extranjero, bien porque, como se ha indicado, lo natural en la nube es la subcontratación"[712]. Y es que el modelo de negocio adoptado por la mayoría de los proveedores de servicios cloud conlleva que los datos sean almacenados y transferidos entre varias jurisdicciones[713].

Por último, la industria[714] recuerda en la misma línea, que las operaciones de los proveedores pueden tener lugar en múltiples ubicaciones al mismo tiempo. Los clientes tienen que ser conscientes también de que más de un proveedor puede verse envuelto a la hora de prestar el servicio en un lugar determinado. Por ejemplo -en el que probablemente es el caso más habitual- un proveedor puede haber facilitado SaaS mientras que otro provee la plataforma o infraestructura en el que se ejecuta.

63. Disponible en web: https://www.researchgate.net/publication/228166466_Data_Export_in_Cloud_Computing_-_How_Can_Personal_Data_Be_Transferred_Outside_the_Eea_The_Cloud_of_Unknowing_Part_4

[711] *Idem.* p. 32.

[712] COTINO HUESO, L. Algunas cuestiones clave de protección de datos en la nube: hacia una regulación nebulosa. *Revista Catalana de Dret Public*. 2015. nº 51. p 85-103.

[713] BURNETT, R. Cloud computing and data protection. *Icaew.* p. 13-15. Disponible en web: https://www.icaew.com/-/media/corporate/files/technical/information-technology/chartech/articles/cloud-computing-and-data-protection.ashx

En todo caso, como apuntan los profesores Hon y Millard conviene aclarar que en la mayoría de los casos, los datos son copiados o replicados en diferentes centros de datos por razones de continuidad del negocio o de recuperación o backup. Además, la primera copia de un conjunto de datos (por ejemplo para un usuario específico o para una aplicación SaaS específica) normalmente se almacena en el mismo centro de datos. Esto será típicamente en el más cercano geográficamente al usuario en cuestión, por cuestiones de latencia (rapidez en el acceso y respuesta a los usuarios), aunque quizá los datos puedan ser almacenados en fragmentos distribuidos entre diferentes hardware de almacenamiento en el mismo centro de datos. De hecho hay quienes señalan que este este sistema es mucho más potente que la disociación o la anonimización de los datos, ya que la dispersión de datos fragmentados en diferentes países permitiría eludir la figura de la transferencia internacional de datos. En el caso de la disociación, los datos no podrían ser relacionados con las personas a las que van referidos, pero seguirían siendo datos inteligibles, con información suficiente, en algunos casos, para asociarlos a los afectados. En la fragmentación no existiría este riesgo, ya que cada fragmento incluiría datos ininteligibles.

Además, en la disociación, el tratamiento se realiza normalmente en bloque, y el proveedor tiene acceso inteligente a todos los datos. En cambio, en la fragmentación, el proveedor sólo tiene un acceso no inteligente a una parte de la base de datos. Es un acceso no inteligente porque se trata de un mero almacenamiento de bits no inteligibles y porque el proveedor no realizará ningún esfuerzo intelectual para tratar los datos. Ver Prodasur. Resumen noticias de actualidad en protección de datos y Boletín LOPD en la empresa. 2012. Disponible en web: http://www.edorteam.net/RESUMEN%20NOTICIAS%20LOPD%202012.pdf

[714] CLOUD SELECT INDUSTRY GROUP (C-SIG). Data Protection Code of Conduct for Cloud Service Providers. ob. Cit.

1.2 Las transferencias internacionales de datos

La primera cuestión a analizar es qué debemos entender por transferencia internacional de datos. Ni la Directiva, ni la LOPD[715], ni el RGPD, tan profuso en definiciones en su art. 4, nos dan una definición propiamente dicha de transferencia internacional. No obstante, sí lo hace el artículo 5.1.s) ROPD que la define como "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 tercero establecido en territorio español". Con base en lo ya tratado en el capítulo anterior, será esta última la que más nos interesa. Desde el punto de vista doctrinal, la profesora Matus Arenas señala que una transferencia internacional como un tratamiento que consiste en la transmisión o transporte de datos, fuera de un Estado, realizado por el responsable del tratamiento directamente a una persona natural (física) o jurídica, que los recibirá en un tercer país, para someterlos a un nuevo tratamiento de datos, bien sea por cuenta propia o por cuenta del transmitente de los datos[716].

Así, por tanto, desde el punto de vista geográfico y con base en lo expuesto, cuando el tratamiento de los datos de un responsable establecido en territorio del espacio económico europeo se lleve a cabo por un encargado o proveedor situado en ese mismo territorio, en ningún caso podremos hablar de transferencia internacional de datos. Sin embargo, nos podemos encontrar ante cualquier de estas otras circunstancias.

[715] Esta habla de "movimiento internacional de datos", que a juicio de la profesora Navas Navarro, comprende "no sólo la transferencia a terceros países, sino también las transferencias a otros países de la UE o a aquellos Estados con un nivel adecuado de protección. NAVAS NAVARRO, S. Computación en la nube: Big Data y protección de datos personales. Ob. cit.

[716] MATUS ARENAS, J. Transferencias internacionales a países con niveles adecuados y no adecuados de protección. Aspectos prácticos. *Seminario Regional de Protección de Datos*. Montevideo, Uruguay. 1 a 4 de junio de 2010. Disponible en web: http://www.redipd.es/actividades/seminario_2010/common/ponencias/Ponencia_J_Matus.pdf

Espacio Económico Europeo	Tercer país
Cliente (responsable)	Proveedor (encargado)
Proveedor (encargado)	Proveedor (subencargado)
Tercer país	Tercer país
Proveedor (encargado)	Proveedor (subencargado)
Proveedor (subencargado)	Proveedor (subencargado)

Fuente: elaboración propia

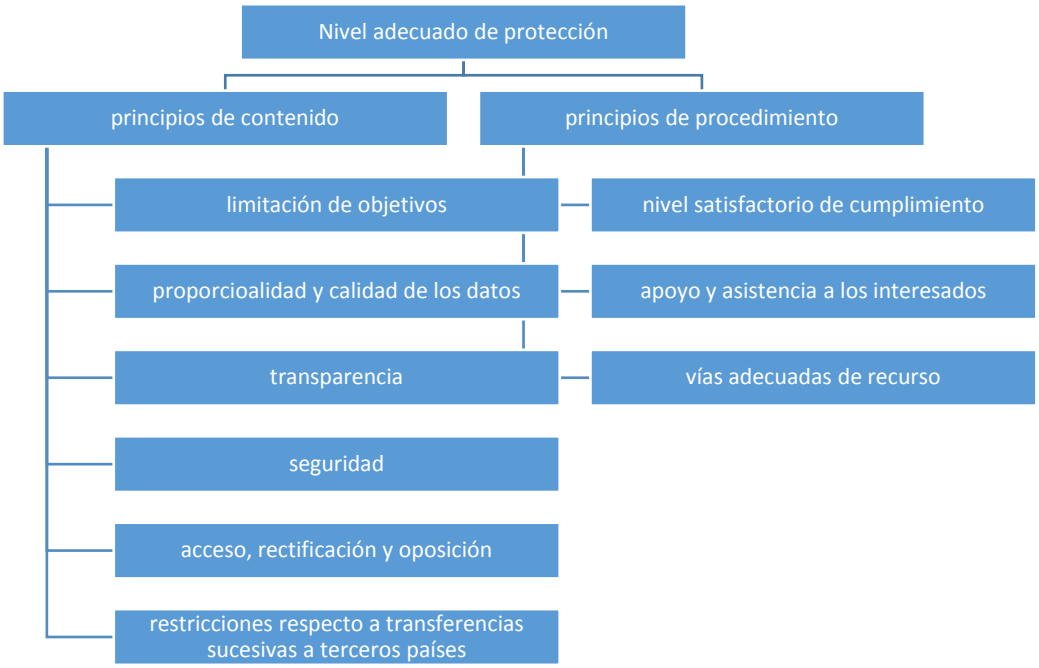
Entrando ya en el régimen jurídico, si hay un elemento vertebrador de las transferencias internacionales de datos o de los flujos transfronterizos de los mismos, es el del nivel equivalente de protección, concepto que como vamos a ver es genéricamente utilizado a la hora de considerar que la transferencia es acorde o no con la legalidad vigente. Se trata de un concepto relativamente antiguo. Así el Convenio 108 del Consejo de Europa, en su artículo 12 señala que "Una Parte no podrá, con el fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte". La regla general por tanto era –en un entorno mucho más permisivo que el actual– la de permitir esas transferencias. Sin embargo, inmediatamente añade en su apartado 3, que "cualquier Parte tendrá la facultad de establecer una excepción a las disposiciones del párrafo 2: a) En la medida en que su legislación prevea una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados de datos de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación de la otra Parte establezca **una protección equivalente**". De similar forma las Directrices de las Naciones Unidas para la regulación de los archivos de datos personales informatizados de 1990, recoge en el punto 9 que "Cuando la legislación de dos o más países afectados por un flujo transfronterizo de datos ofrezca **salvaguardas similares** para la protección de la intimidad,

la información debe poder circular tan libremente como dentro de cada uno de los territorios afectados. En caso de que no existan salvaguardas recíprocas, no deberán imponerse limitaciones indebidas a tal circulación, sino solamente en la medida en que lo exija la protección de la intimidad"[717]. En fin, el artículo 25.1 de la Directiva 95/46 nos dice que "Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un **nivel de protección adecuado**". Encontramos referencias a este concepto incluso en alguna de las escasas normas que en el Derecho Comparado contempla disposiciones específicas concernientes a la nube. Así, en México, el artículo 63 de la Ley General de Protección de Datos personales en posesión de sujetos obligados, en su versión de 26 de enero de 2017, dice: "El responsable podrá contratar o adherirse a servicios, aplicaciones e infraestructura en el cómputo en la nube, y otras materias que impliquen el tratamiento de datos personales, **siempre y cuando el proveedor externo garantice políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la presente Ley** y demás disposiciones que resulten aplicables en la materia".

¿Y qué debe entenderse por un nivel de protección adecuado? Con base en lo apuntado ya en el año 1998 por el Grupo de Trabajo del artículo 29, se debe basar, de manera simplificada, en dos elementos: el contenido de las normas aplicables y los medios para asegurar su aplicación eficaz[718].

[717] NACIONES UNIDAS. Directrices para la regulación de los archivos de datos personales informatizados. 14 de diciembre de1990. Disponible en web: http://inicio.ifai.org.mx/Estudios/D.3BIS-cp--Directrices-de-Protecci-oo-n-de-Datos-de-la-ONU.pdf

[718] GRUPO DE TRBAJO DEL ARTÍCULO 29. Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE. 1998. Disponible en web: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_es.pdf



Fuente: elaboración propia con base en el Grupo de Trabajo del artículo 29

En el RGPD, el tratamiento de esta cuestión merece un capítulo propio, en concreto su Capítulo V. Comienza con el principio general antes señalado, que en este caso viene a situar en un mismo plano al responsable y al encargado, por cuanto a ambos se dirige a la hora de subrayar la necesidad de cumplir con las condiciones establecidas en dicho capítulo y en particular el asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado. Se concretan diferentes modalidades para lograrlo: la transferencia basada en una decisión de adecuación; la autorización otorgada por una autoridad de control; las normas corporativas vinculantes, conocidas por su acrónimo inglés BCR; las cláusulas contractuales tipo; un código de conducta y el mecanismo de certificación.

1.2.1 La transferencia basada en una decisión de adecuación[719].

Se trata del supuesto en el que un determinado territorio garantiza un nivel adecuado de protección. A diferencia de lo que venía siendo habitual, con el RGPD la decisión adoptada

[719] A día de hoy las decisiones de adecuación vigentes con terceros países son:
- **Suiza.** Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000

por la Comisión Europea ya no estará pensada en un país, sino también en un territorio o en uno o varios sectores específicos de un país, además de una organización internacional. Esta primera consideración plantea varias dudas ¿qué se debe entender por territorio? ¿Qué se debe entender por "sector específico"?[720] En cuanto al concepto de territorio, que responde tradicionalmente a una delimitación física, pero con una proyección jurídico constitucional, parecería estar pensando en conceptos como el de región, estado, departamento, es decir divisiones territoriales que tienen una sustantividad política o administrativa reconocible en el seno de un país.

Mayor interés si cabe a nuestros efectos tiene el término "sector específico", por cuanto los proveedores de servicios cloud pueden encajar perfectamente dentro de dicho concepto. Pensemos a estos efectos por ejemplo en la *Cloud Computing Association* en el caso de Estados Unidos[721] o, como la más conocida, la *Cloud Security Alliance* que, como ya se ha visto en otras partes de este capítulo, goza de reconocimiento e interlocución con la Comisión Europea[722]. Se trata en todo caso de un mecanismo que se asemeja mucho, en el componente subjetivo, a los códigos de conducta o los mecanismos de certificación, tal y como se estudiará en otra parte de este capítulo.

En todo caso, el aparente cambio ya no es tan sustancial porque este componente sectorial no deja de estar vertebrado en torno al concepto territorial, y porque el redactado del artículo habla de uno o varios sectores de "ese tercer país". Pero es que además, los elementos o

---

- **Canadá.** Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos.
- **Argentina**. Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003
- **Guernsey**. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003
- **Isla de Man.** Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004
- **Jersey.** Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008
- **Islas Feroe.** Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010
- **Andorra.** Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010
- **Israel.** Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011
- **Uruguay.** Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012
- **Nueva Zelanda.** Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012

[720] Responde parcialmente esta referencia al sector a algunas críticas que se habían vertido a la redacción de la Directiva por parte de determinados sectores doctrinales. Así, los profesores Hon y Millard señalaban en 2012 que "la redacción de la Directiva de protección de datos no ha previsto la posibilidad de que los datos exportados pudieran ser adecuadamente protegidos por otros medios como por ejemplo una encriptación potente u otras medidas adoptadas por el responsable/exportador o el receptor/importador. HON, K., MILLARD, C. y MILLARD, C. Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the Eea? The Cloud of Unknowing, ob. Cit. p. 33.

[721] http://www.cloudcomputingassn.org/index.html

[722] https://cloudsecurityalliance.org/

parámetros a atender por parte de la Comisión a la hora de adoptar la decisión y que se reflejan en el siguiente cuadro, no se entenderían sin dicho elemento territorial:

el Estado de Derecho,
los derechos fundamentales,
la legislación pertinente,
el acceso de las autoridades públicas a los datos personales,
las normas de protección de datos,
las normas profesionales y las medidas de seguridad,
las normas sobre transferencias ulteriores de datos personales,
la jurisprudencia,
los derechos de los interesados
los recursos.
el funcionamiento efectivo de una o varias autoridades de control independientes
los compromisos internacionales en relación con la protección de los datos personales.

Fuente: elaboración propia con base en el art. 45.2 RGPD

Todos los elementos que se contemplan o se analizan lo están referidos a un país y buena prueba de ello es cómo en el propio redactado del apartado 2 del art. 45 se mencionan exclusivamente a los países y a las organizaciones internacionales, excluyendo los conceptos de territorio y de sectores específicos antes citados. No podemos sino atribuir esto al hecho de que en los sectores específicos se verán en todo casos caracterizados por los referidos elementos, al margen de prácticas, códigos de conducta u otros elementos que individualicen al sector específico y que supongan un elemento añadido. En el caso de los territorios, no se encuentra justificación por cuanto pueden tener normas específicas en materia de protección de datos para cuyo examen entendemos se deberán utilizar elementos de similar naturaleza.

Especial mención hay que hacer en este punto, ya no solo por su repercusión en el mercado del cloud, sino por su particularidad frente a otras decisiones de adecuación, al denominado

Acuerdo de puerto seguro[723] que permitía las transferencias internacionales de datos a las empresas norteamericanas adheridas o comprometidas con dicho mecanismo. Cabe recordar al respecto que el TJUE tuvo la oportunidad de pronunciarse sobre esta cuestión de manera rotunda con motivo de su Sentencia de 6 de octubre de 2015, en la que afirmó que "para que se considere que un país otorga un nivel adecuado de protección su ordenamiento jurídico deberá establecer un nivel de garantías "*esencialmente equivalente*" al establecido en la Unión Europea, ya que sólo así se garantizan suficientemente los derechos fundamentales"[724]. En todo caso dicho acuerdo se ha visto sustituido por el denominado "Privacy Shield" que resultó objeto de aprobación el 12 de julio de 2016[725].

[723] Este fue adoptado 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 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. El acceso al texto completo del mismo en el siguiente enlace;: https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/decisiones/common/pdfs/B.12-cp--Decisi-oo-n--sobre-la-adecuaci-oo-n-conferida-por-los-principios-de-puerto-seguro.pdf

[724] Unión Europea. Tribunal de Justicia de la Unión Europea (Gran Sala). Caso Maximillian Schrems vs. Data Protection Commissioner (C-362/14)). Sentencia de 6 de octubre de 2015. Acceso completo al texto de la sentencia en el siguiente enlace: http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=ES

Un buen comentario a la sentencia, ALVAREZ CARO, M. Análisis de la sentencia de invalidez del acuerdo de puerto seguro (*safe harbour*). *Revista de Privacidad y Derecho Digital*. abril 2016. nº 3. p.73-110. Por otro lado, como guía durante la situación de interinidad, sirvan las adecuadas observaciones de la autoridad británica, INFORMATION COMMISSIONER'S OFFICE. Data transfers to the US and Safe Harbor – interim guidance. 10 de febrero de 2016. De hecho cabe señalar cómo la autoridad holandesa de protección de datos ya había puesto de manifiesto la actuación que tiene que llevar a cabo el responsable a la hora de verificar el cumplimiento de la normativa en las transacciones internacionales en el seno de contratos cloud con un proveedor americano. En concreto sus conclusiones en el año 2012 fueron las siguientes: "El cumplimiento con los principios del Acuerdo de Puerto seguro por sí mismo no garantiza que la organización está adherida a ellos en la práctica. El responsable deberá asegurarse que la certificación existe y que se cumple en la práctica. Incluso si se demuestra que se cumple con dichos principios, eso significa simplemente que la transferencia de datos personales a los Estados Unidos puede tener lugar y no que el tratamiento en los Estados Unidos cumpla con todas las exigencias de la Directiva 95/46. No hay ninguna garantía de que el tratamiento en los Estados Unidos cumpla los requerimientos exigidos por la ley nacional aplicable a través de la que se ha implementado la Directiva 95/46. Incluso cuando el tratamiento es realizado por un encargado, así como en el caso del tratamiento en la nube, el responsable sigue siendo responsable del cumplimiento con esta ley. El responsable por tanto deberá asegurarse, en la firma del contrato, que todas las previsiones normativas aplicables están cubiertas, y que tendrá también que asegurarse que cualquier acuerdo adicional se incorpora al contrato".

WET BESCHERMING PERSOONGEGEVENS. Written opinion on the application of the in the case of a contract for cloud computing services from an American provider**.** 2012. Disponible en web: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/dutch-dpa-written-opinion-cloud-computing-unofficial-translation.pdf

Las autoridades americanas han sido particularmente críticas con estos posicionamientos de sus colegas europeos. Buena pruebo de ello es el siguiente documento: US DEPARTMENT OF COMMERCE'S INTERNATIONAL TRADE ADMINISTRATION (ITA) Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing. Disponible en web: https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2013/04/Safe-Harbor-and-Cloud-Computing-Clarification_April-12-2013_Latest_eg_main_060351.pdf

[725] EUROPEAN COMMISSION. Commission implementing decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy

Sobre esta cuestión volveremos más adelante cuando tratemos el acceso a la información en la nube por parte de las autoridades públicas, elemento que estuvo en el punto de partida de la anulación del Acuerdo de Puerto Seguro.

Las decisiones de adecuación tienen en todo caso un carácter dinámico y están continuamente sometidas a un escrutinio, ya no solo por las autoridades judiciales, tal y como ocurrió con el caso Schrems, sino por parte de las autoridades que las aprueban. Así, los tres últimos apartados del art. 45 contemplan un mecanismo de supervisión continua por parte de la Comisión Europea y un mecanismo de revisión al menos cada cuatro años, que habilitará en su caso para una anulación, modificación o suspensión del correspondiente acto de ejecución. Como ha demostrado el desarrollo de la propia tecnología del cloud computing, la velocidad del desarrollo tecnológico hace particularmente aconsejable estos mecanismos.

1.2.2 La autorización otorgada por una autoridad de control.

En ausencia de una decisión de adecuación, las transferencias por parte del responsable o del encargado (la referencia a este último como veremos posteriormente es de particular relevancia en el entorno del *cloud computing*) solamente podrán hacerse si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

En este caso las garantías vendrán dadas, conforme a lo previsto en el art. 46.3 RGPD, mediante la aportación de las cláusulas suscritas en el correspondiente contrato entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales, debiendo aplicarse el mecanismo de coherencia previsto en los arts. 63 y siguientes del RGPD. Cabe señalar que serán susceptibles de ser utilizados a estos efectos los mismos parámetros que los anteriormente mencionados por cuanto son los que ponen de manifiesto las garantías necesarias para la protección de los derechos de los interesados. Igualmente se debe subrayar que nos siguen resultando de interés las previsiones del art. 37.3 ROPD, donde se contemplan las causas de exclusión o de suspensión de los contratos por parte del Director, en este caso, de la AEPD: a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos

Shield. COM (2016) 4176 final, 12 de julio de 2016. Disponible en web: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf

que el contrato garantiza; b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo; c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador; d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos; e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados.

En cuanto a los aspectos procedimentales, los arts. 137 a 140 ROPD contemplan el procedimiento de autorización propiamente dicho y hacen recaer la actitud proactiva en el exportador de los datos, que en nuestro caso y con base en la actual redacción del RGPD, recuérdese, puede ser tanto el cliente (en el supuesto de un proveedor situado en un país tercero), como el propio proveedor (cuando este se encuentre en territorio español pero lo subcontrate con un proveedor situado en un país tercero). El exportador, además de los requisitos legales, deberá aportar: la identificación del fichero o ficheros a cuyos datos se refiera la transferencia internacional (ficheros que desaparecen con el RGPD), con indicación de su denominación y código de inscripción del fichero en el Registro General de Protección de Datos; la transferencia o transferencias respecto de las que se solicita la autorización, con indicación de la finalidad que la justifica; y la documentación que incorpore las garantías exigibles para la obtención de la autorización así como el cumplimiento de los requisitos legales necesarios para la realización de la transferencia, en su caso. A ello se añade la aportación de la copia del contrato cuando sea este el fundamento de la transferencia, así como las normas o reglas adoptadas en relación con el tratamiento de los datos en el seno de un grupo, así como la documentación que acredite su carácter vinculante y su eficacia dentro del grupo. Igualmente deberá aportarse la documentación que acredite la posibilidad de que el afectado o la propia Agencia puedan exigir la responsabilidad que corresponda en caso de perjuicio del afectado o vulneración de las normas de protección de datos por parte de cualquier empresa importadora.

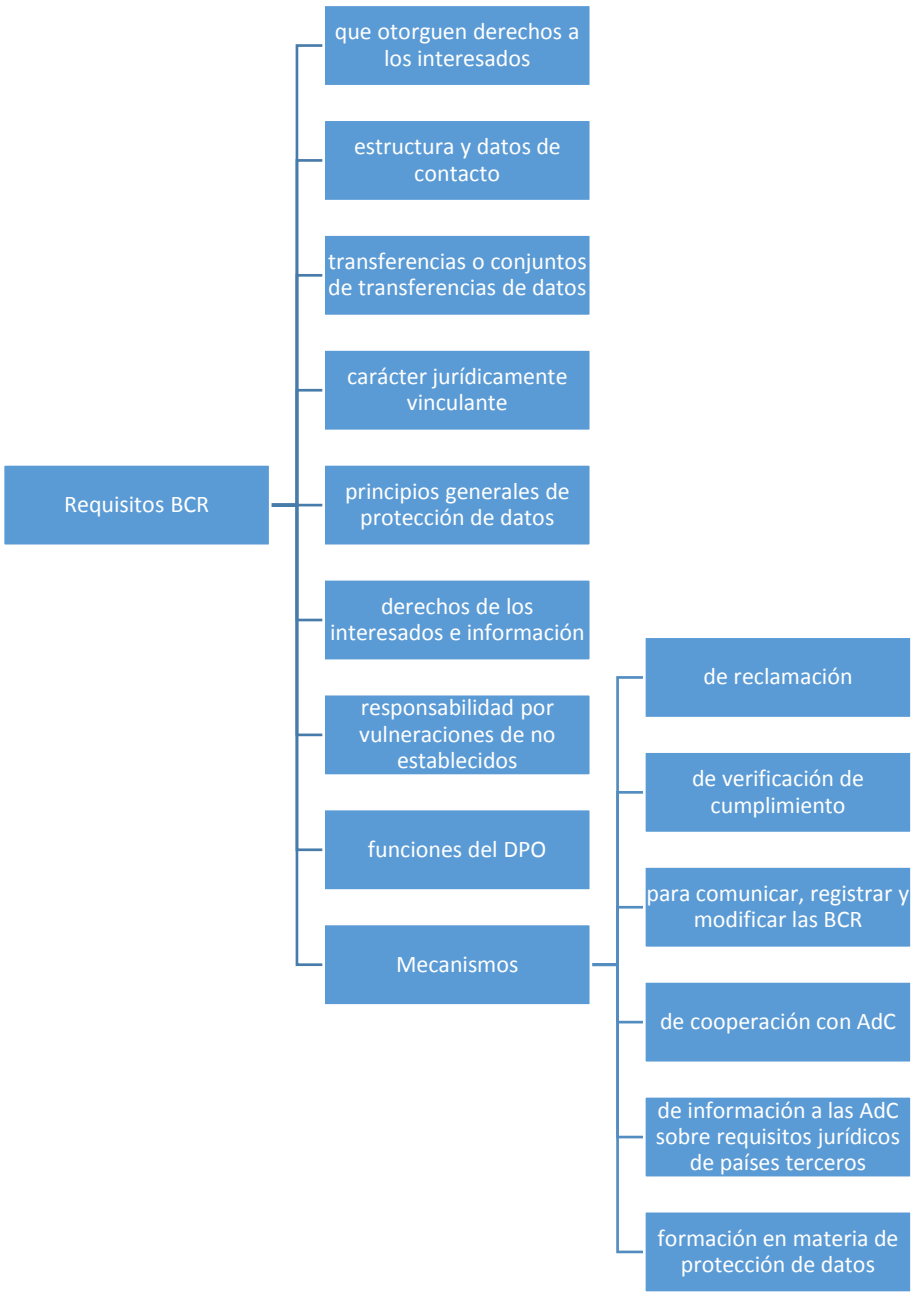
A pesar de las disposiciones normativas, la propia Agencia, en su sitio Web, es todavía más detallista al señalar que en el caso de una transferencia a un importador/encargado que es necesario que el contrato esté firmado por las partes (copia original o fotocopia compulsada) y, en su caso, traducción jurada al español; así como poderes suficientes de los firmantes y, en su caso, traducción jurada al español. En el caso de que nos encontremos con el supuesto de importador/subencargado, además de los citados requisitos, será necesario el contrato

marco entre el responsable del tratamiento y el encargado del tratamiento/exportador de datos en el que se autorice a éste la subcontratación y la transferencia internacional de datos y, en su caso, traducción jurada al español. En el campo de la subcontratación profundizaremos posteriormente por la trascendencia que tiene en nuestro ámbito de estudio.

1.2.3 Las normas corporativas vinculantes, conocidas por su acrónimo inglés BCR[726].

Es también el art. 46 RGPD, en este caso en el apartado 2, el que contempla que las garantías adecuadas podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por las denominadas BCR. Estas a su vez son tratadas en el art. 47 RGPD donde se sientan los requisitos de las mismas. Desde el punto de vista formal y como su propia denominación indica, la característica básica es que han de ser jurídicamente vinculantes (art. 47.1.a) y en cuanto a su contenido se recoge que como mínimo ha de ser el siguiente:

[726] Son muy abundantes los dictámenes emitidos por el Grupo de Trabajo del artículo 29 respecto a las BCR:
- WP 155 - Preguntas más frecuentes sobre BCRs.
– WP 154 - Cuadro que establece la estructura de las BCRs.
– WP 153 - Cuadro que establece la relación de los elementos y principios que deben contener las BCRs.
– WP 108 - Modelo de solicitud de autorización de transferencia internacional basada en BCRs en el ámbito del procedimiento coordinado.
– WP 107 - Documento sobre la competencia de las Autoridades de Control europeas en el procedimiento coordinado de aprobación las BCRs.
– WP- 74 - Documento sobre la aplicación del artículo 26.2 de la Directiva 95/46/CE a las BCRs.



Fuente: elaboración propia

En todo caso, por el importante papel que como veremos pueden jugar en el campo de la subcontratación con base en el RGPD, las desarrollaremos posteriormente.

1.2.4 Las cláusulas contractuales tipo

Otro supuesto al margen de la decisión de adecuación pero que permite una transferencia internacional, es el de las cláusulas tipo de protección de datos. En este caso nos encontramos ante un contrato tipo como los ya existentes bajo cuyo paraguas se puede llevar a cabo la transferencia. Como señala el Grupo de Trabajo del artículo 29 para que una cláusula contractual pueda cumplir la función garantista, debe compensar de manera satisfactoria la ausencia de una protección general adecuada mediante inclusión de los elementos esenciales de la misma que no existen en una situación determinada[727].

Con base en los apartados c) y d) del art. 46.2 RGPD, pueden ser adoptadas por la Comisión o bien adoptadas por una autoridad nacional de protección de datos y aprobadas por la Comisión. En realidad, una interpretación correcta de esta última afirmación es que va a ser la Comisión Europea la que proceda a su aprobación en todo caso. El procedimiento previsto al efecto es el denominado procedimiento de examen que desarrolla el art. 5 del Reglamento (UE) nº 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por por la Comisión[728]. Estas cláusulas cumplen una cuádruple función: facilitadora,

[727] GRUPO DE TRABAJO DEL ARTÍCULO 29. Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE. 1998. Disponible en web: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_es.pdf

[728] El referido artículo, reza como sigue: *Artículo 5*
Procedimiento de examen
1. Cuando se aplique el procedimiento de examen, el comité emitirá su dictamen por la mayoría prevista en el artículo 16, apartados 4 y 5, del Tratado de la Unión Europea y, cuando proceda, en el artículo 238, apartado 3, del TFUE, para los actos que deban adoptarse a partir de una propuesta de la Comisión. Los votos de los representantes de los Estados miembros en el comité se ponderarán del modo establecido en dichos artículos.
2. Cuando el comité emita un dictamen favorable, la Comisión adoptará el proyecto de acto de ejecución.
3. Sin perjuicio de lo dispuesto en el artículo 7, si el comité emite un dictamen no favorable, la Comisión no adoptará el proyecto de acto de ejecución. Cuando se considere necesario un acto de ejecución, el presidente podrá, bien presentar al mismo comité una versión modificada del proyecto de acto de ejecución en el plazo de dos meses a partir de la emisión del dictamen no favorable, bien presentar al comité de apelación para una nueva deliberación el proyecto de acto de ejecución en el plazo de un mes a partir de dicha emisión.
4. En ausencia de dictamen, la Comisión podrá adoptar el proyecto de acto de ejecución, salvo en los casos contemplados en el párrafo segundo. Si la Comisión no adopta el proyecto de acto de ejecución, el presidente podrá presentar al comité una versión modificada del mismo.
Sin perjuicio de lo dispuesto en el artículo 7, la Comisión no adoptará el proyecto de acto de ejecución cuando:
a)dicho acto se refiera a la fiscalidad, los servicios financieros, la protección de la salud o la seguridad de las personas, los animales o las plantas, o medidas de salvaguardia multilaterales definitivas;
b)el acto de base establezca que el proyecto de acto de ejecución no podrá ser adoptado si no se ha emitido un dictamen, o

supletoria, de flexibilidad y de garantía[729], siendo esta última la relevante a los efectos que nos ocupa.

Llama la atención en este punto la previsión del Considerando 109 en el que se subraya que nada impide la posibilidad de que se añadan nuevas cláusulas "siempre que no contradigan, directa o indirectamente, las cláusulas contractuales tipo adoptadas por la Comisión o por una autoridad de control, ni mermen los derechos o las libertades fundamentales de los interesados". Y de hecho añaden que "Se debe alentar a los responsables y encargados del tratamiento a ofrecer garantías adicionales mediante compromisos contractuales que complementen las cláusulas tipo de protección de datos".

Existen en este punto, a día de hoy, dos modelos de cláusulas que están basadas en los respectivos esquemas de transferencias internacionales de datos: responsable a responsable, en cuyo caso serán de aplicación las Decisiones de la Comisión Europea 2001/497/CE, de 15 de junio de 2001, y 2004/915/CE, de 27 de diciembre de 2004, por la que se modifica la anterior; o bien la transferencia de responsable a encargado del tratamiento, en cuyo caso serán de aplicación las cláusulas contractuales tipo establecidas en la Decisión de la Comisión Europea 2010/87/UE, de 5 de febrero de 2010. En este punto, y en el ámbito concreto del cloud computing, merece la pena detenerse en el Informe 0157/2012 [730] en el que se planteaban dos cuestiones concretas relacionadas con la aplicación a los contratos que pudieran celebrarse en el futuro de las cláusulas contractuales tipo aprobadas mediante la Decisión de la Comisión 2010/87/UE, y que se vieron reflejadas

c) se oponga a ello una mayoría simple de los miembros que componen el comité.
En cualquiera de los casos mencionados en el párrafo segundo, cuando se considere necesario un acto de ejecución, el presidente podrá, bien presentar al mismo comité una versión modificada del mismo en el plazo de dos meses a partir de la votación, bien presentar al comité de apelación para una nueva deliberación el proyecto de acto de ejecución en el plazo de un mes a partir de la votación.
5. No obstante lo dispuesto en el apartado 4, se aplicará el siguiente procedimiento para la adopción de proyectos de medidas antidumping o compensatorias definitivas en los casos en que el comité no haya emitido un dictamen y una mayoría simple de los miembros que lo componen se oponga al proyecto de acto de ejecución.
La Comisión realizará consultas con los Estados miembros. A los 14 días como muy pronto y al mes como muy tarde de la reunión del comité, la Comisión informará a los miembros de los resultados de esas consultas y presentará un proyecto de acto de ejecución al comité de apelación. No obstante lo dispuesto en el artículo 3, apartado 7, el comité de apelación se reunirá a los 14 días como muy pronto y al mes como muy tarde de la presentación del proyecto de acto de ejecución. El comité de apelación emitirá su dictamen con arreglo al artículo 6. Los plazos establecidos en el presente apartado se entenderán sin perjuicio de la obligación de respetar los plazos fijados en los actos de base pertinentes.

[729] SANCHO VILLA. D. Negocios internacionales de Tratamiento de datos personales", Thomson Reuters, Civitas, Cizur Menor. 270 p.

[730] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Informe 0157/2012. Disponible en web: https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2012-0157_Especialistas-cl-aa-usulas-contractuales-en-cloud-computing..pdf

luego también en otros expedientes concretos[731]. Se trataba de un supuesto en el que, con la finalidad de amoldar el clausulado general a la computación en nube, se planteaba la posibilidad de modificar dos cláusulas de las establecidas por la Comisión Europea. Al respecto, la Agencia señaló en sus conclusiones que las modificaciones planteadas en el modelo establecido por la Decisión impedirían entender las cláusulas resultantes como amparadas en el citado modelo. Sin embargo, añadía que las garantías en relación con las citadas modificaciones podrían considerarse adecuadas para amparar una transferencia internacional de datos derivada de la contratación de los servicios de computación en nube que la misma presta, siendo posible que se solicitase del Director de la Agencia la adopción de una Resolución de autorización de transferencia internacional de datos de carácter personal sobre la base de las garantías derivadas de las citadas modificaciones.

No se contemplan sin embargo en el ámbito europeo la existencia de cláusulas contractuales tipo para los supuestos de transferencias internacionales de datos entre un proveedor de servicios en nube radicado en el Espacio Económico Europeo y un subencargado fuera de dicho espacio. Por su implicación para la computación en nube, en la que con frecuencia se produce este fenómeno, resulta muy relevante recordar que la AEPD aprobó en su Autorización de Transferencia Internacional de Datos de 16 de octubre de 2012 unas cláusulas contractuales tipo para las transferencias Internacionales de datos de encargado a subencargado del tratamiento[732]. Como afirma Cotino Hueso, se necesitan determinadas adaptaciones del entorno de la nube (para evitar tener diferentes contratos por cliente entre un proveedor y sus subencargados), lo que podría implicar la necesidad de una autorización previa de la autoridad de protección de datos competente. La ventaja para las empresas de servicios de nube españolas es que, si se logra la autorización de transferencia de datos

[731] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Expediente TI/00032/2014 Agencia Española de Protección de Datos, "Resolución de declaración de adecuación de garantías para las transferencias internacionales de datos a los Estados Unidos con motivo de la prestación de servicios de computación en nube", 9 de mayo de 2014, https://on.uclm.es/pdf/TI-00032-2014_Resolucion-de-fecha-09-05-2014_de-MICROSOFT-CORPORATION_a-Estados-Unidos.pdf

[732] http://www.faura-casas.com/wp-content/uploads/2014/06/Resolucion.pdf
Hay que tener en cuenta que la Decisión de 2010, tal y como recoge su Considerando 23, "La presente Decisión solo se aplica a la subcontratación por un encargado del tratamiento establecido en un tercer país de sus servicios de tratamiento a un subencargado establecido en un tercer país, por lo que no se aplicará a la situación en la que un encargado del tratamiento establecido en la Unión Europea y que realice el tratamiento de datos personales en nombre de un responsable del tratamiento establecido en la Unión Europea subcontrate sus operaciones de tratamiento a un subencargado del tratamiento establecido en un tercer país. En tales situaciones, los Estados miembros son libres de tener en cuenta el hecho de que los principios y las garantías de las cláusulas contractuales tipo establecidas en la presente Decisión se hayan utilizado para subcontratar a un subencargado establecido en un tercer país con la intención de prestar la adecuada protección de los derechos de aquellos interesados cuyos datos personales se estén transfiriendo para operaciones de subtratamiento".

siguiendo estas cláusulas contractuales, no se precisa en general una ulterior si se mantiene lo establecido en el contrato. Solo tendrán que notificar —no pedir autorización— cada nueva transferencia internacional para que esta quede registrada[733].

Este modelo, como señala Emmanuelle Bartoli, se ha mostrado sumamente útil a efectos de ser utilizado también como esquema general a nivel europeo[734]. La AEPD lo ha venido extendiendo, como se pone de manifiesto en el Informe "*Utilización del Cloud Computing por los despachos de abogados y el derecho a la protección de datos de carácter personal*"[735]. Por su parte, el Grupo de Trabajo del art. 29 elaboró en el año 2014 un documento de trabajo que incluye precisamente un borrador de cláusulas para cubrir las transferencias internacionales entre un encargado del tratamiento dentro del Espacio Económico Europeo y un subencargado en un tercer país[736]. El borrador de cláusulas está precisamente basado en las elaboradas por la autoridad española[737]. Siguiendo las líneas marcadas por Oliver Proust podemos señalar cuáles son las principales características de estas cláusulas:

- Estructura: la totalidad de la estructura y el contenido de las cláusulas son similares a las ya utilizadas en las cláusulas responsable-encargado, sin perjuicio de su correspondiente adaptación.
- Contrato marco: el encargado debe firmar un contrato marco con el responsable que recoge una lista de obligaciones (dieciséis en total) especificadas en el borrador y que incluye restricciones a posteriores subtratamientos. El efecto práctico de esto podría ser ver que los términos de servicio entre responsables y sus encargados en territorio UE se expandieran para incluir un sustancial mayor número de obligaciones en materia de protección de datos, destinados todos ellos a facilitar futuras

[733] COTINO HUESO, L. Algunas cuestiones clave de protección de datos en la nube: hacia una regulación nebulosa. Ob. cit. p. 99.
[734] BARTOLI, E. Data transfers in the cloud. *Expert Group on Cloud Computing Contracts. European Commission*. 28 de marzo de 2014. Disponible en web: http://ec.europa.eu/justice/contract/files/expert_groups/discussion_paper_data_transfers_in_cloud.pdf
[735] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Utilización del Cloud Computing por los despachos de abogados y derecho a la protección de datos de carácter personal. 2012. Disponible en web: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2012/notas_prensa/common/junio/informe_CLOUD.pdf
[736] ARTICLE 29 DATA PROTECTION WORKING PARTY. Working document 01/2014 on Draft Ad hoc contractual clauses "EU data processor to non-EU sub-processor". 2014. Disponible en web: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp214_en.pdf
[737] PROUST, O. Article 29 Working Party issues draft model clauses for processor-to-subprocessor data transfers. *Privacylawblog*. 9 de abril de 2014. Disponible en web: http://privacylawblog.fieldfisher.com/2014/article-29-working-party-issues-draft-model-clauses-for-processor-to-subprocessor-data-transfers/

transferencias por parte del encargado a los subencargados bajo estas cláusulas modelo.

- Subtratamiento. El encargado europeo deberá obtener, tal y como desarrollaremos con más detalle posteriormente a la hora de tratar la subcontratación, el consentimiento previo por escrito del responsable para poder subcontratar a encargados fuera del territorio UE. Corresponderá en todo caso al responsable decidir, bajo el contrato marco, si otorga un consentimiento general para todas las actividades de subtratamiento o si requiere de una autorización caso por caso. En todo caso el subencargado estará jurídicamente vinculado por las mismas obligaciones (en particular medidas técnicas y organizativas) como las impuestas al encargado bajo el contrato marco.
- Listado de acuerdos de subtratamiento: el encargado deberá mantener una lista actualizada de todos los acuerdos de subtratamiento suscritos y ponerla a disposición del responsable.
- Cláusula del tercero beneficiario: en función de la situación, el interesado tiene tres opciones para hacer cumplir las vulneraciones de la cláusula modelo: contra el encargado exportador de los datos; el encargado importador fuera de la UE o cualquiera de los subencargados.
- Auditorías: el encargado exportador de los datos debe acordar, a solicitud el responsable, someterse a una auditoría del responsable respecto de las actividades de tratamiento cubiertas bajo el contrato marco o, alternativamente, un órgano de inspección independiente seleccionado por el responsable. Este último punto, que fue particularmente debatido en el informe 0157/2012 de la Agencia al que hemos hecho mención y que suponía una modificación de las más trascendentes de las cláusulas de 2010, es especialmente relevante para la industria cloud quien, por razones operativas y de seguridad, será particularmente renuente a que sean los clientes los que lleven a cabo la auditoría in situ, pero que se sentirán mucho más cómodos sometiéndose a auditorías de terceros independientes.
- Transparencia del contrato marco: el responsable debe poner a disposición de los interesados y de la autoridad competente, cuando se le solicite, una copia del contrato marco y cualquier acuerdo de subtratamiento con la excepción de la información comercial sensible que podrá eliminarse. En la práctica señala Oliver Proust, es cuestionable cuántos *partners* estarán dispuestos a firmar acuerdos de subtratamiento con encargados europeos sobre la base de que las previsiones de

dichos acuerdos podrían acabar siendo desveladas a los reguladores y otros terceros.

- Conclusión del acuerdo marco: cuando el encargado/exportador/proveedor de servicios en nube, el encargado importador o cualquier subencargado incumpla sus obligaciones, el responsable podrá suspender la transferencia de datos y/o resolver el contrato.

A pesar de que estas cláusulas están pendientes de aprobación, y aunque en el caso concreto de España disponemos de la referida Resolución de Autorización de Transferencia Internacional de Datos de 16 de octubre de 2012, el RGPD sí ha introducido una importante novedad. Como ya se ha señalado, al hablar de las transferencias internacionales, el legislador europeo ya no está pensando exclusivamente en que las mismas se lleven a cabo entre un responsable radicado en territorio del EEE y un encargado o un responsable situado fuera de dicho territorio. El art. 46.1 RGPD, en el marco de la regulación de la transferencia internacional de datos, habla de que "el responsable *o el encargado* del tratamiento solo podrá transmitir datos personales a un tercer país…". Esto supone no solamente la permisividad para dictar unas cláusulas contractuales tipo sino un verdadero mandato para que la Comisión adopte dichas cláusulas, que resultarán de particular interés para el entorno del *cloud computing*.

1.2.5 Un Código de conducta y el mecanismo de certificación

Por sus similitudes en el ámbito de las transferencias internacionales de datos, se tratan conjuntamente. En el caso de los códigos de conducta, se trata de uno de los mecanismos que, si bien ya contemplados en la normativa europea (art. 27 de la Directiva) y en la española (art. 32 LOPD) se ven claramente impulsados por el RGPD por la amplitud de materias que pueden ser objeto de regulación y cuya adhesión puede servir como instrumento de cumplimiento con diversos requisitos del RGPD.

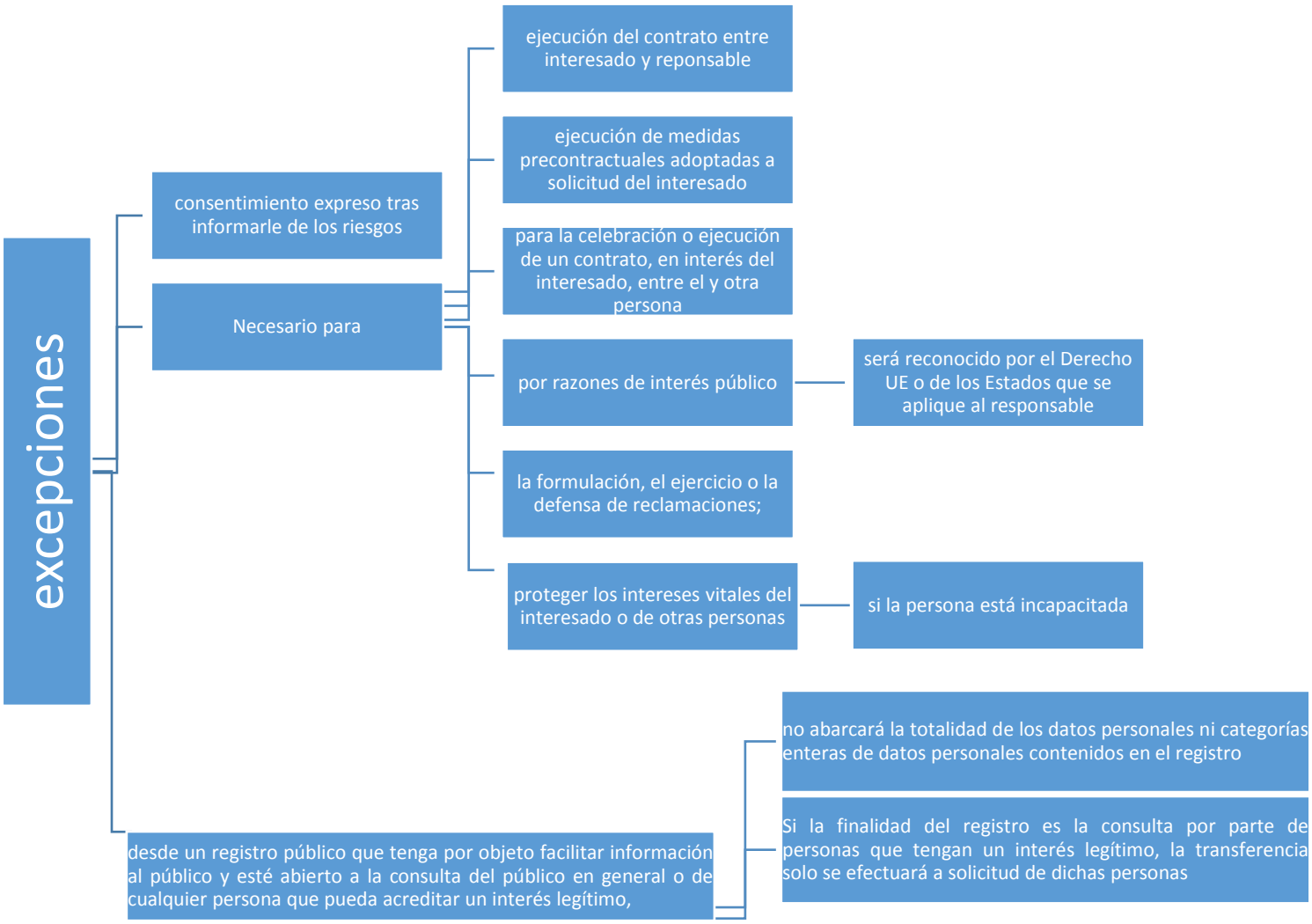
En el campo que nos ocupa, tiene una particular incidencia en el ámbito de las transferencias internacionales de datos. Como señala el art. 40.3, además de la adhesión de los responsables o encargados del tratamiento a los que se aplica el RGPD, los responsables o encargados a los que no se aplica pueden adherirse también a códigos de conducta aprobados, a fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales. En todo caso, apunta el

citado artículo y en lo que nos ocupa, el proveedor deberá asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados. Este último inciso es igualmente subrayado por el artículo 46.2.e). Idénticas previsiones se recogen respecto a los mecanismos de certificación, tanto en lo que se refiere a su aplicabilidad a proveedores o encargados a los que inicialmente no se aplicaría (art. 42.2 RGPD) como en lo concerniente a las exigencias de compromiso jurídico (art. 46.2.f) RGPD).

Esta redacción, a nuestro juicio desvirtúa en sí mismo el mecanismo del código de conducta y el de certificación, y nos lleva ante una mezcla de los supuestos anteriormente mencionados. Por un lado, los códigos o certificaciones en sí mismas han de ser autorizados ex art. 40 por una autoridad de control o por la Comisión para la extensión de la validez general al territorio UE. Ello en sí mismo parece lógico. Sin embargo, la adhesión por parte del proveedor a un código o a un mecanismo de certificación, aprobado por las referidas autoridades y que ofrece suficientes garantías, parece no compadecerse con la necesidad añadida de asumir compromisos jurídicamente vinculantes y exigibles. De hecho, una exigencia de este tipo, en realidad desvirtúa -o al menos empequeñece- la utilidad de estos instrumentos.

1.2.6 Excepciones

Hasta ahora se ha hablado de los diversos mecanismos que existen para salvaguardar la existencia de un “nivel equivalente de protección”. Sin embargo, no debemos olvidar, además de todo lo dicho, la existencia de determinadas excepciones a las reglas anteriormente expuestas. Como se refleja en el siguiente gráfico, solamente se podrá dar la transferencia internacional si:



Fuente: elaboración propia con base en el art. 49 RGPD

Los Considerandos nos ayudan en la interpretación de algunos de los conceptos indeterminados utilizados en el RGPD y que se reflejan en la figura de arriba. Así, el -Considerando 112 recoge, de manera no exhaustiva, las razones importantes de interés público: intercambios internacionales de datos entre autoridades en el ámbito de la competencia, administraciones fiscales o aduaneras, entre autoridades de supervisión financiera, entre servicios competentes en materia de seguridad social o de sanidad pública, por ejemplo, en caso contactos destinados a localizar enfermedades contagiosas o para reducir y/o eliminar el dopaje en el deporte

Si ninguno de los supuestos descritos resulta aplicable, entonces el apartado 2 del citado artículo contempla que solamente podrá llevarse a cabo la transferencia internacional de datos: si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías adecuadas con respecto a la protección de datos personales. Además, el propio cliente o el proveedor de servicios documentarán en los registros tanto la evaluación como las garantías adecuadas.

En este caso el cliente de la nube deberá informar a la autoridad de control y, además de sus obligaciones de información genéricas, deberá informar al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos.

Por último, como excepción al régimen planteado, en ausencia de una decisión el Derecho de la Unión o de los Estados podrá, por razones importantes de interés público, establecer expresamente límites a la transferencia de categorías específicas de datos a un tercer país, lo cual se deberá notificar a la Comisión.

Con base en lo tratado en este subapartado, podemos concluir que el RGPD articula un sistema de transferencias internacionales muy similar al existente, basado en el concepto de nivel equiparable de protección e incluso con alguna modulación que resulta de particular interés para la computación en nube, caso del concepto de sector específico. A ello se añaden fórmulas como las de los modelos de clausulado estandarizado, que podrían articularse específicamente para el negocio de la computación en nube, o los códigos de conducta y los mecanismos de certificación. Todos ellos son instrumentos que resultarían facilitadores del tráfico económico y de la seguridad jurídica para proveedores, clientes y, lógicamente, para la salvaguarda del derecho fundamental a la protección de datos de los interesados.

1.3 Subcontratación

1.3.1 La subcontratación en el ADN de la nube

En el marco de las transferencias internacionales de datos, y aunque no está recogida esta terminología en el RGPD ni tampoco en el de la LOPD, básicamente existen dos sujetos: el exportador y el importador de los datos. De nuevo el ROPD nos ayuda con las definiciones

y así en su art. 5.1.g), dice que el exportador es "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"; mientras que define al importador en la letra ñ) como "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".

Nótese que, aunque se pueda producir con una cierta frecuencia, estos conceptos, como ya hemos resaltado, no tienen por qué ser equivalentes a los de responsable y encargado del tratamiento o, en nuestro caso, a los de cliente y proveedor de servicios en nube. Y es que ya hemos apuntado al principio de este apartado que el fenómeno de la subcontratación es particularmente relevante en el entorno cloud, La asignación de recursos dinámica es un elemento clave de la computación en nube. Es necesario evitar malgastar recursos debido a una infrautilización y del mismo modo es necesario evitar un tiempo de respuesta excesivo como consecuencia de una sobreutilización[738]. A ello sirve el recurrir a terceros a través de la subcontratación. Hoy día la nube es directamente impensable sin la subcontratación[739] porque es la que permite en gran medida cumplir con dos de sus notas más características: la escalabilidad y la elasticidad, significando la primera que los recursos pueden ampliarse o contraerse en función de las necesidades del cliente, y la segunda que esa expansión o contracción se puede hacer rápidamente[740].

Pero sin duda esta realidad no está exenta de riesgos. Como reflejara ya la ENISA en 2009 al margen de los problemas o de la necesaria atención a la articulación jurídica de la cadena de subcontrataciones, existen también riesgos desde el punto de vista de la seguridad en el servicio. En concreto la ENISA habla del "fallo en la cadena de suministro" y señala que "el nivel de seguridad del proveedor en nube puede estar supeditado al nivel de seguridad de cada enlace y al grado de dependencia de terceros del proveedor en nube. Cualquier interrupción o corrupción de la cadena, así como la falta de coordinación de las

[738] YAZIR, Y.O, MATTHEWS, C., FARAHBOD, R., NEVILLE, S., GUITOUNI, A. GANTI, S., COAD, Y., Dynamic Resource Allocation in Computing Clouds using Distributed Multiple Criteria Decision Analysis. In: *Proceeding of IEEE 3rd International Conference on Cloud Computing*. 2010. p. 91–98.
[739] CONRAD, I., DOVAS, M-U., POGGIOLLI, F., SELK, R., y WOLFGRAM, S. Cloud Computing Contracts – Discussion Paper on Subcontracting. *European Commission.* 25 de marzo de 2014. Disponible en web: http://ec.europa.eu/justice/contract/files/expert_groups/expert_group_subcontracting_discussion_paper_en.pdf
[740] CHANG, H. Data protection regulation and cloud computing, En CHEUNG, A.S.Y. y WEBER, R.H. (eds). *Privacy and Legal Issues in Cloud Computing*. Elgar Publishing. 2015. 333 p.

responsabilidades entre las partes implicadas puede ocasionar: la no disponibilidad de los servicios, la pérdida de la confidencialidad, la integridad y la disponibilidad de los datos, las pérdidas económicas y de renombre debidas a la incapacidad de cumplir las demandas del cliente, el incumplimiento de los Acuerdos de nivel de servicio, el fallo en el servicio de conexión en cascada, etc."[741].

A esta perspectiva tan relevante y que está en el propio ADN del servicio cloud, se añade también la perspectiva económica, por cuanto los bajos costes de infraestructura que algunos proveedores ofrecen, favorecen la aparición de innovadores servicios, particularmente en el modelo SaaS ofrecido por pequeñas empresas[742].

Recogida su importancia desde el punto de vista tecnológico y de tejido económico, sin embargo en el plano jurídico la subcontratación es determinante de algunos de los principales riesgos que se le achacan a la nube: la falta de transparencia y la pérdida de control, ya que la relación de subcontratación del proveedor es muy probablemente invisible al usuario de la nube [743]. Como recuerda la Agencia, puede haber una cadena de subcontrataciones -que algunos llaman caja negra[744]- que en teoría podría no tener fin, y cuyo objeto, como acabamos de apuntar, es redimensionar continuamente los recursos de la nube de forma dinámica y en función de las condiciones del mercado[745]. De similar modo, el Grupo de Trabajo del artículo 29 señala que los dos grandes riesgos en la nube son: la ausencia de control sobre los datos personales, así como una información insuficiente respecto a cómo, dónde y por quién están siendo tratados o subtratados los datos[746]. En fin, la CNIL afirma que uno de los principales riesgos de la computación en nube es el fallo en la cadena de subcontrataciones cuando el proveedor haya recurrido a ellas para prestar el servicio[747]. Prueba de la preocupación sobre el aspecto referido a la falta de transparencia

[741] ENISA. Beneficios, riesgos y recomendaciones para la seguridad de la información. Ob. Cit. p. 35.
[742] CUESTA SAINZ, C., ALONSO, J., TUESTA, D. y FERNÁNDEZ DE LIS, S. El desarrollo de la industria del cloud computing: impactos y transformaciones en marcha. *Observatorio de Economía Digital. BBVA Research.* 2014. Disponible en web: https://www.bbvaresearch.com/wp-content/uploads/2014/07/Observatorio-Econom%C3%ADa-Digotal_040714.pdf
[743] BUYYA, R., BROBERG, J. y GOSCINSKY, A.M. *Cloud Computing: Principles and Paradigms*. Willey. 2011. 664 p.
[744] MILLER, R. y WHITTEN, T. Subcontratación segura en la nube: cinco preguntas clave que hay que formular. *CA Technologies.* 2012. p. 3. Disponible en web: http://www.ca.com/es/~/media/Files/whitepapers/ca-securely-outsourcing-to-the-cloud-wp-esn.pdf
[745] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía para clientes que contraten servicios de Computing. Ob. cit. p. 9.
[746] ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 5/2012, on Cloud computing. p. 9.
[747] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. Recommendations for companies planning to use Cloud computing services. Disponible en web:

es cómo el artículo 64.I.b) de la Ley General de Protección de Datos Personales en posesión de sujetos obligados de México define el cómputo en la nube (versión de 26 de enero de 2017) señala que "Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor: I. Cumpla, al menos, con lo siguiente: **b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio**".

En el plano doctrinal también se ha destacado este riesgo. Así, Chang subraya que el principal riesgo de la subcontratación radica en la pérdida de control[748]. En nuestro país, Marzo Portera recuerda que "es una obviedad que el hecho mismo de que exista una cadena de subcontrataciones transfronteriza aumenta la problemática relativa a la pérdida del control sobre los distintos subcontratistas, su identificación, lugar de residencia…"[749].

Como no podía ser de otro modo, la industria no hace referencia a que nos encontremos ante un riesgo, pero sabe de la importancia de este elemento, y así *European Privacy Seals,* a título de ejemplo, lo considera como uno de los aspectos más relevantes del cloud[750].

1.3.2 El proveedor fuera del Espacio Económico Europeo

La regulación actual contempla el fenómeno de la subcontratación de manera genérica. En concreto, recoge -en el artículo 21 ROPD- que el encargado, el proveedor, no puede subcontratar la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que contase con su autorización, contratándolo entonces en nombre y por cuenta del responsable del tratamiento. A pesar de ello y conforme al apartado 2 de ese mismo artículo, no será necesaria la autorización siempre que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar. Si no resulta posible, deberá comunicar al responsable los datos que la identifiquen antes de proceder a la subcontratación.

https://www.cnil.fr/sites/default/files/typo/document/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf

[748] CHANG, H. Data protection regulation and cloud computing, En CHEUNG, A.S.Y. y WEBER, R.H. (eds). *Privacy and Legal Issues in Cloud Computing*. Elgar Publishing. 2015. 333 p.

[749] MARZO PORTERA, A.M. Privacidad y cloud computing, hacia dónde camina Europa. Ob. cit. p. 221.

[750] EUROPE PRIVACY SEALS. Cloud Computing and European Data Protection Law. 2012.

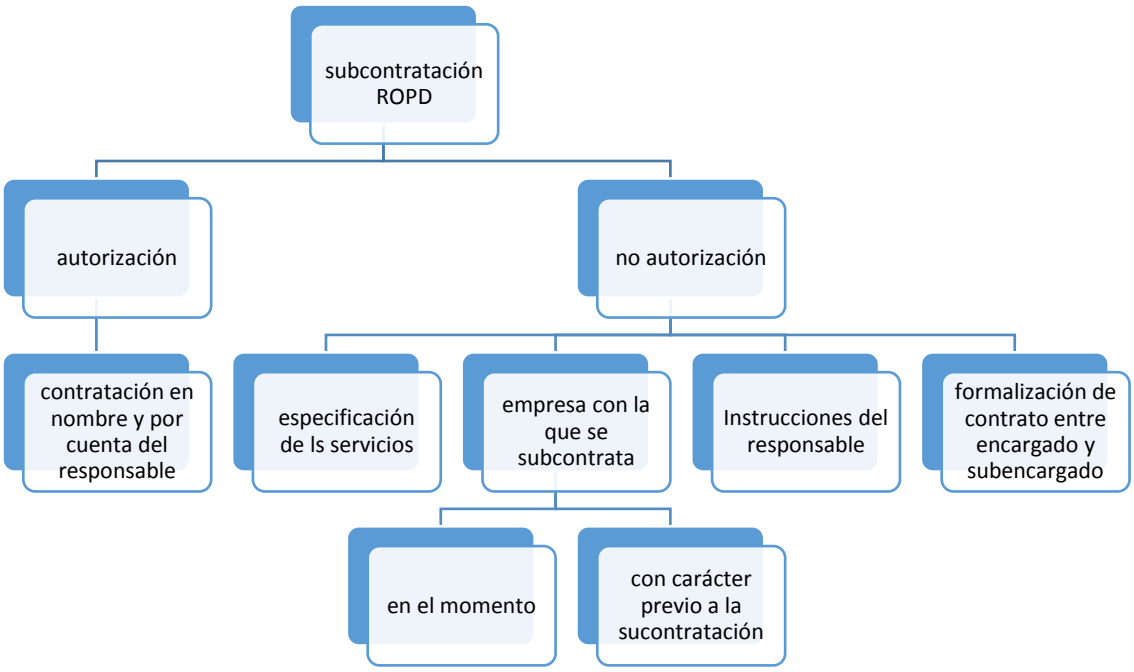
Por tanto, el elemento clave radica bien en la autorización expresa o bien articulando elementos que permitan la posibilidad de conocer quién va en definitiva a tratar los datos. Como señala la Agencia en el Informe 582/2004[751] "El fundamento de dicha previsión se deriva directamente de la propia naturaleza del derecho fundamental a la protección de datos de carácter personal. En este sentido, si dicho derecho consiste, según indica el Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre, en un poder de disposición del afectado sobre la información que le concierne, resulta lógico que, habiendo autorizado (o habiendo previsto la Ley) que los datos puedan ser objeto de tratamiento por parte de un determinado responsable, será preciso que dicho responsable conozca en cada momento qué terceras entidades acceden a dichos datos, siempre en su nombre, a fin de garantizar al interesado que los datos de los que el mismo es titular no excedan del control de aquella entidad cuyo tratamiento ha sido aceptado por aquél" y continúa señalando que "Si se estableciera la posibilidad de subcontratar sucesivamente dicho tratamiento sin conocimiento del responsable, éste carecería de conocimiento para poder atender cualquier reclamación efectuada por el afectado e incluso para conocer quién accede en cada momento a los datos de carácter personal cuyo tratamiento ha sido consentido por el interesado".

Además, hemos señalado, el proveedor de cloud debe asumir en el contrato que los subcontratistas le ofrecen garantías jurídicas para el tratamiento de los datos equivalentes a los que él mismo asume. Por ello, las exigencias de nuestro Reglamento no radican exclusivamente en el conocimiento o la identificabilidad sino que el tratamiento en todo caso se tendrá que ajustar a las instrucciones del responsable, y el contrato entre el encargado y el subcontratista deberá ajustarse a las mismas características que el contrato entre responsable y encargado. Precisamente, de todos estos requisitos, el punto de las instrucciones ha sido particularmente recalcado por el Grupo de Trabajo del art. 29 que afirma que "No hay nada en la Directiva que impida que, por exigencias organizativas, se pueda designar a varias entidades como encargadas (o subencargadas) del tratamiento de datos, incluso subdividiendo los cometidos en cuestión. Ahora bien, todas ellas tienen que ajustarse a las instrucciones dadas por el responsable del tratamiento de los datos al llevar a cabo el tratamiento"[752]. En este punto, no faltan quienes sostienen que los prestadores de

[751] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Informe 582/2004. Disponible en web: https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/transferencias_internacionales/common/pdfs/2004-0582_Subcontrataci-oo-n-de-un-encargado-del-tratamiento-en-tercer-pais-que-no-ofrece-nivel-adecuado-de-protecci-oo-n.pdf

[752] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento". Disponible en web: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

servicios cloud no tratan los datos de manera directa con base en las instrucciones del cliente, sino que son los clientes quienes directamente utilizan los servicios cloud, por ejemplo, subiendo datos, editándolos o borrándolos. No tendría sentido entonces hablar de seguir las instrucciones del responsable. Con base en el caso Salems[753] se sostiene que el seguimiento de las instrucciones del cliente tiene como finalidad evitar un uso no autorizado o la revelación de datos personales por parte del proveedor[754].



Fuente: elaboración propia

De las dos opciones que permite nuestro actual ROPD Rubí Navarrete subraya que la primera no es apropiada para la nube por las rigideces a las que está sometida en la práctica, que señala son tanto de índole formal (acreditación de la representación, en muchas ocasiones en idiomas distintos y en países diversos) y material (limitación en el poder decisión sobre el uso de los datos que corresponde al responsable del tratamiento)[755]; y es

[753] DAVIS, S. Sweden's Data Protection Authority bans Google http://www.privacysurgeon.org/blog/incision/swedens-data-protection-authority-bans-google-apps/
[754] HON, W.K. GDPR: Killing cloud quickly? *International Association of Privacy Professionals (IAPP).* 17 de marzo de 2016. Disponible en web: https://iapp.org/news/a/gdpr-killing-cloud-quickly/
[755] RUBÍ NAVARRETE, J. El proveedor de cloud como encargado del tratamiento. En MARTINEZ MARTÍNEZ R., Derecho y Cloud Computing. Civitas Thomson-Reuters. 2012. p. 87-107.

por ello que existe una tendencia generalizada a focalizarse en el segundo de los mecanismos, que goza de una mayor flexibilidad si tenemos en cuenta que no exige propiamente de una autorización.

En lo que nos concierne, esta solución conlleva que el proveedor de cloud computing tiene que informar al cliente sobre la tipología de servicios que pueden subcontratarse con terceros, al menos delimitando genéricamente los servicios en los que participarán (alojamiento, capacidad de procesamiento…etc), y a su vez el cliente tiene que dar su conformidad. Pero además deberá indicar la empresa concreta con la que subcontrata, bien sea en el momento de celebrar el contrato con el responsable, bien identificándola al responsable con carácter previo a su contratación, permitiendo al cliente por tanto que se oponga.

A pesar de que este es un sistema más flexible y consiguientemente más ajustado a la computación en nube, no deja de plantear dificultades. Como recuerda Javier Ribas, el proceso de selección de las empresas que el proveedor de cloud computing contrata está basado en las oscilaciones de la oferta de servicios como el almacenamiento de datos, y por lo tanto está sujeto a una evolución constante[756]. Añade Rubí Navarrete en la misma línea, que efectivamente el proveedor suele incorporar un abanico de entidades subcontratadas y puede tener la necesidad de incorporar otras o sustituirlas con flexibilidad. Además, continúa el mismo autor, los responsables pueden ser igualmente muy variados como para que se pronuncien sobre la idoneidad de dichos subcontratistas[757]. De hecho, el Tribunal Supremo, en su Sentencia de 15 de julio de 2010, puso de manifiesto la importancia de estas obligaciones y más concretamente, la obligación de que el encargado del tratamiento comunique al responsable la necesidad de subcontratar y con quién pretende hacerlo. Hay que tener en cuenta, como apunta la ENISA[758], que "Si un proveedor no declara los servicios básicos de TI que están subcontratados —no es realista que los proveedores indiquen los contratistas utilizados, puesto que estos pueden cambiar con frecuencia—, el cliente no está en situación de evaluar de manera adecuada el riesgo al que se enfrenta. Esta falta de transparencia puede reducir el nivel de confianza en el proveedor". Lo cierto es que, al igual que en otros muchos aspectos de la nube y teniendo en cuenta el tamaño en muchas ocasiones de proveedor y cliente, resulta poco realista que se establezca esta suerte de

[756] RIBAS, J. La subcontratación en el cloud computing. *Expansión.* 24 de mayo de 2012. Disponible en web: http://www.expansion.com/blogs/ribas/2012/05/24/la-subcontratacion-en-el-cloud-computing.html
[757] RUBI NAVARRETE, J. ob. cit. p. 104.
[758] ENISA. Beneficios, riesgos y recomendaciones para la seguridad de la información. Ob. cit. p. 36.

control por parte del cliente respecto a las actividades subcontratadas por parte del proveedor[759].

Siendo consciente de ello, la Agencia ha recogido un criterio de flexibilidad y subraya que, considerando que el cliente tiene que poder conocer los terceros que intervienen en el tratamiento, se puede satisfacer de una manera dinámica, por ejemplo pudiendo acceder a una página web o a través de otras opciones que le facilite el prestador del servicio. La utilización de este sistema de actualización a través de la web reúne la doble condición de otorgar la seguridad jurídica que el cliente quiere, y permitir la flexibilidad necesaria que el servicio exige. Con este criterio estamos asistiendo a una modulación razonable de lo previsto en el artículo 21 y satisfaciendo, cierto es que con un nivel de diligencia "in vigilando", el fundamento último de las previsiones normativas allí establecidas.

En el plano normativo, y teniendo en cuenta que la existencia de la subcontratación, como hemos mencionado al principio de este capítulo, hace todavía más factible que concurra el fenómeno de las transferencias internacionales, es conveniente observar también el régimen jurídico de estas en el ámbito concreto de la subcontratación. Así, la Decisión de la Comisión de 5 de febrero de 2010 recoge en su Considerando 17 que "… debe establecer las condiciones que ha de cumplir el subtratamiento para garantizar que los datos personales que se están transfiriendo sigan protegidos con independencia de la sucesiva transferencia a un subencargado del tratamiento". En concreto, la cláusula 11 exige el previo consentimiento por escrito del exportador de datos. Si el importador de datos subcontrata sus obligaciones con arreglo a las cláusulas, con el consentimiento del exportador de datos, lo hará exclusivamente mediante un acuerdo escrito con el subencargado del tratamiento de datos, en el que se le impongan a este las mismas obligaciones impuestas al importador de datos con arreglo a las cláusulas. En los casos en que el subencargado del tratamiento de datos no pueda cumplir sus obligaciones de protección de los datos con arreglo a dicho acuerdo escrito, el importador de datos seguirá siendo plenamente responsable frente al exportador de datos del cumplimiento de las obligaciones del subencargado del tratamiento de datos con arreglo a dicho acuerdo".

Está asunción de responsabilidad se pone de manifiesto en el apartado 2 de la misma cláusula, al señalar que el contrato escrito previo entre el importador de datos y el

[759] MLEX. Cloud computing: obligations under the Directive v. GDPR. Junio de 2016. Disponible en web: http://www.mmlex.it/wp-content/uploads/2016/09/DPLP-June-2016-Cloud-Computing.pdf

subencargado del tratamiento contendrá asimismo una cláusula de tercero beneficiario, para los casos en que el interesado no pueda interponer la demanda de indemnización contra el exportador de datos o el importador de datos por haber estos desaparecido de facto, cesado de existir jurídicamente o ser insolventes, y ninguna entidad sucesora haya asumido la totalidad de las obligaciones jurídicas del exportador de datos o del importador de datos en virtud de ley o contrato. Dicha responsabilidad civil en todo caso está limitada por cuanto el subencargado la verá limitada a sus propias operaciones de tratamiento[760].

En la misma línea que se ha visto más arriba, cuando se ha descrito sucintamente el régimen jurídico del borrador de cláusulas para las transferencias entre encargado y subencargado, el último apartado de la citada cláusula 11 recoge que el exportador de datos conservará la lista de los acuerdos de subtratamiento celebrados en una lista que se actualizará al menos una vez al año y que se pondrá a disposición de la autoridad de control de protección de datos del exportador/cliente/responsable.

Debemos tener en cuenta, como ya se ha transcrito más arriba, que esta Decisión, como bien explica el Considerando 23 "…solo se aplica a la subcontratación por un encargado del tratamiento establecido en un tercer país de sus servicios de tratamiento a un subencargado establecido en un tercer país, por lo que no se aplicará a la situación en la que un encargado del tratamiento establecido en la Unión Europea y que realice el tratamiento de datos personales en nombre de un responsable del tratamiento establecido en la Unión Europea subcontrate sus operaciones de tratamiento a un subencargado del tratamiento establecido en un tercer país".

El RGPD ha recogido en línea continuista con lo que anteriormente se ha señalado, en cuanto a los requisitos de identificabilidad y de seguimiento de las instrucciones. Se dice así que el encargado no recurrirá a un subencargado sin la autorización previa por escrito del

[760] Más allá del régimen de la protección de datos, existen lo que se llaman los acuerdos "back to back" que implican que los proveedores de la nube, en tanto que parte directamente responsable frente al cliente, deben trasladar no solamente los aspectos técnicos y comerciales de los que son responsables a los subcontratistas, sino también los aspectos jurídicos, en particular la exposición a la responsabilidad. Si no lo hacen, el proveedor se puede encontrar en la situación en la que es responsable ante el cliente por disfuncionalidades o daños que son, de hecho, responsabilidad del subcontratista y el proveedor no tendría recurso para repercutir estos costes al subcontratista. REEDSMITH. Transcending the Cloud: A Legal Guide to the Risks and Rewards of Cloud Computing. Cloud Computing-A German Perspective. Disponible en web: https://www.reedsmith.com/files/Publication/cf6df614-498c-4c92-979c-454346c15369/Presentation/PublicationAttachment/131ec3c6-65ff-45e4-bca1-f5628e478465/Cloud%20Computing%20-%20Germany%20Chapter%20ONLY%20-%2008.12.10.pdf

responsable sea específica o general. En todo caso, cualquier cambio previsto en dichos subencargados, deberá ser notificado por el encargado al responsable, permitiendo a este la posibilidad de oponerse (art. 28.2). Parece por tanto que hay una suerte de combinación de las dos vías antes apuntadas, una más formalista con autorización específica, y otra en la que cabe entender una autorización general de los servicios en el contrato marco pero con capacidad de oposición por parte del cliente a los subcontratistas concretos. Además, el prestador de servicios cloud tendrá que imponer mediante contrato u otro acto jurídico las mismas obligaciones de protección de datos que las estipuladas en el contrato entre el cliente y el proveedor (art. 28.4). De hecho, el prestador de servicios en nube se juega mucho en estas disposiciones por cuanto será él el que responda ante el responsable del tratamiento, ante el cliente, en el caso de incumplimiento de las obligaciones por parte del subencargado.

La particularidad del fenómeno de la subcontratación en el ámbito cloud y las dificultades que se dan para la adaptación de algunas de las cláusulas previstas en la citada Decisión de 2010 se pusieron de manifiesto en el igualmente mencionado Informe 0157/2012[761] -en muchos aspectos reiterado en el Informe 0464/2012[762]- en el que la Agencia se planteaba dos cuestiones de la que nos ocupa la segunda, concerniente a si la importadora podría firmar con los subcontratistas un único contrato que se refiriese a la totalidad de los servicios que la importadora hubiera ya contratado o pudiera contratar en el futuro. Hay que recordar que la cláusula 11 contempla la necesidad de un acuerdo escrito con el subencargado. La Agencia –al igual que otras como la alemana–[763] tal y como ya hemos apuntado, señala en este informe que, siempre que el cliente del servicio de computación en nube pueda tener claro conocimiento de la identidad de los terceros subcontratistas del servicio, así como de las actividades desplegadas por cada uno de ellos, nada obsta a que la citada subcontratación se realice mediante la firma de un único contrato con dichos subcontratistas en que se especifiquen los servicios a prestar. Ello debería acompañarse de un

[761] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Informe 0157/2012.
[762] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Informe 0464/2012. Disponible en web: https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2012-0464_Contrataci-oo-n-de-servicio-de-cloud-computing-por-cl-ii-nica-m-ee-dica.pdf
[763] SCHUPPERT, S. German DPAs Issue Rules for Cloud Computing Use. *Chronicle of Data Protection. Hogan Lovells.* 13 de octubre de 2011. Disponible en web: http://www.hldataprotection.com/2011/10/articles/international-eu-privacy/german-dpas-issue-rules-for-cloud-computing-use/
La versión actualizada de la guía en alemán, se puede encontrar en:
DER KONFERENZ DERE DATENSCHUTZBEAUFTRAGTEN DES BUNDES UND DER LÄNDER SOWIE DER ARBEITSGRUPPE INTERNATIONALER DATENVEKEHR DES DÜSSELDORFER KREISSES. Orientierungshilfe – Cloud Computing. 9 de octubre de 2014. Disponible en web: https://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf

procedimiento que permitiera a los clientes acceder a los citados datos de identificación, para lo que sería suficiente a efectos de acreditar la existencia de garantías adecuadas que los clientes pudieran acceder, por ejemplo a través de un sitio web al que se hiciera expresa referencia en el contrato firmado con la importadora, a los datos de identificación de los subcontratistas, ubicación de los mismos y servicios de tratamiento que aquéllos desarrollarán, bastando la celebración de un contrato único con tales subcontratistas que, lógicamente cumpliese con los requisitos necesarios para que cupiera atribuir a los mismos la condición de subencargados del tratamiento o para adoptar garantías suficientes en caso de transferencia ulterior de los datos. En definitiva, lo que está señalando la Agencia, en línea con lo que luego recogería en su Guía y que se ha descrito más arriba, es la necesidad de transparencia en identificación y labor desarrollada, dando una vía por la cual la misma se puede lograr. Esta misma postura se ha adoptado en otros países. Así, en el caso de Alemania, se considera igualmente que se cumplen los requisitos de la subcontratación si el proveedor mantiene una lista online de acceso protegido respecto de los subencargados que recoja el nombre y la dirección del subencargado, así como una breve descripción de los servicios prestados, sin perjuicio de que pueda requerir al proveedor que le facilite los términos del contrato suscrito con el mismo en lo concerniente a la protección de datos[764].

Cabe subrayar al respecto que esta política de transparencia ha sido una de las más reforzadas con el RGPD que ha incorporado el principio de transparencia expresamente como uno de los principios que han de regir el tratamiento de los datos (art. 5.1.a)) y que en el Considerando 39 se dice que exige que toda información y comunicación relativa al tratamiento de datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Y además esa transparencia ha de informar la totalidad de la cadena y de los sujetos involucrados. Fernández Aller[765] habla de un "encadenamiento de garantías" para hablar del entramado contractual. Nosotros hablamos de un "encadenamiento de información o de transparencia". La transparencia debe asegurarse vis-à-vis el interesado así como las relaciones entre el cliente, el proveedor y los subcontratistas. La transparencia en la nube, como señala Europe Privacy Seals, significa que es necesario para el cliente de

[764] EUROCLOUD DEUTSCHLAND. Guidelines Cloud Computing German Law, Data Protection & Compliance. 2014. Disponible en web: http://www.cloudingsmes.eu/wordpress/wp-content/uploads/2014/07/EuroCloud_GuidelineLaw-DP-C_EN1.pdf

[765] FERNÁNDEZ ALLER, C. Algunos retos de la protección de datos en la sociedad del conocimiento. Especial detenimiento en la computación en nube (cloud computing). *Revista de derecho UNED*. 2012. nº 10. p. 125-145

la nube ser consciente de todos los subcontratistas y de todas las ubicaciones en las que los datos personales puedan ser almacenados por el proveedor y por los subcontratistas.

En realidad con la solución aportada en dicho informe, estamos ante uno de los ejemplos de progresiva adaptación de la normativa de protección de datos al entorno cloud, cuestión esta en todo caso sobre la que, lógicamente, profundizaremos en las conclusiones de este trabajo[766]. La modificación del clausulado hace que la transferencia ya no fuera posible realizarla al amparo de las cláusulas tipo que establece la Decisión de 2010. Así lo señala el Grupo de Trabajo del artículo 29 en las Q&A referidas a dicha Decisión, al recordar que el Anexo I al contrato sería siempre diferente porque variaría el exportador (nuestro cliente), así como probablemente las categorías de datos, los interesados y la descripción de las operaciones de tratamiento. De similar modo la Agencia, en el referido informe, concluye que no cabe ampararse en la Decisión, pero se subraya igualmente que si un proveedor adoptase unas cláusulas estandarizadas que aun difiriendo de las contenidas en la Decisión 2010/87/CE contuviesen las garantías adecuadas de protección de los derechos de los afectados e introduciendo modificaciones en el tenor de algunas de las cláusulas, como la que hemos mencionado, en los términos ya vistos, sería posible que por parte de la Agencia dictar una resolución determinando que las garantías contenidas en las citadas cláusulas deben considerarse adecuadas a los efectos previstos en el artículo 33.1 LOPD, lo que implicaría una autorización automática de cualquier transferencia internacional realizada al amparo de tales cláusulas en tanto no se produjera ninguna alteración de las mismas, bastando una notificación.

1.3.3 El proveedor en el Espacio Económico Europeo

Hasta aquí hemos tratado el supuesto en el que el prestador de servicios cloud se encuentre radicado en un tercer país. Sin embargo no podemos obviar la posibilidad real de que dicho proveedor se encuentre radicado en territorio español y sin embargo subcontrate los servicios con un importador de datos que, en su condición de subencargado, se encuentre

[766] En la misma línea de adaptabilidad de las cláusulas existentes al entorno cloud, ver OFFICE OF THE INFORMATION COMMISSIONER y THE OFFICE OF THE DATA PROTECTION COMMISSIONER. Cloud Computing A guide for data controllers. Summary of the Article 29 Working Party Opinion (amended to apply to Jersey and Guernsey Law. Disponible en web: https://dataci.je/wp-content/uploads/2016/04/Cloud-Computing_Apr16.pdf

radicado en un país tercero. Este supuesto no ha sido contemplado expresamente por ninguna Decisión comunitaria, ya que como recuerda Kuner, las cláusulas de la Decisión de 2010 cubren las transferencias de la UE a un encargado en un país tercero, pero no de un encargado en la UE a un subencargado fuera de la UE, aunque la autoridad de protección de datos puede autorizar el uso de nuevas cláusulas en dichas situaciones[767]. Cierto es que, como ha señalado el Grupo de Trabajo del artículo 29 en estos casos sería viable también, como opciones, un contrato directo entre el responsable del tratamiento y el subencargado del tercer país, conforme a la Decisión 2010/87/UE, o incluso un mandato expreso por el cual el responsable da al encargado del tratamiento establecido en el EEE el poder de utilizar las cláusulas tipo de la Decisión 2010/87/UE por su cuenta.

En España, la postura que igualmente se venía manteniendo era la de la contratación directa entre el responsable y el subencargado radicado en un tercer país, sin que se admitiera la posibilidad de una contratación entre dos encargados o entre encargado y subencargado y así venía reflejado en el Informe 582/2004 anteriormente citado. Sin embargo ya hemos adelantado que desde 2012 se ha optado por un modelo de clausulado elaborado por la Agencia Española de Protección de Datos[768]. Este modelo recoge una serie de cláusulas que van en la línea de las previstas para una subcontratación "ordinaria" y que quedan reflejadas en la siguiente figura, muy similar, lógicamente, a las del modelo de clausulado que se quedó en fase de borrador en la Comisión Europea:

Aspectos más destacados del clausulado estándar de encargado en España y subencargado en país tercero

[767] KUNER, C. Data Protection and Cloud Computing: an Overview of the Legal Issues. *Nordic IT Law Conference.* Copenhagen. 12 November 2010. Disponible en web: http://it-retsforum.dk/wp-content/uploads/2016/03/Data_Processing_and_Cloud_Computing_by_Christopher_Kuner.pdf

[768] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Modelo de cláusulas contractuales AEPD para transferencias internacionales de datos entre encargado y subencargado del tratamiento. 21 de marzo de 2012. Disponible en web: https://www.agpd.es/portalwebAGPD/resoluciones/autorizacion_transf/common/pdfs/MODELO-DEFINITIVO-AEPD_Contrato-encargado-subencargado-21-03-2012.pdf
Cabe señalar como curiosidad que "en un primer momento el modelo de cláusulas contractuales se mantuvo en secreto por parte de la AEPD. Solo se facilitaría por parte de la Agencia a aquellas entidades que tuvieran un interés real en emplearlas para sus transferencias internacionales de datos. Esta postura cambió completamente a partir de la solicitud de autorización para la transferencia internacional de datos efectuada a 16 de julio de 2012 por una empresa en calidad de encargada del tratamiento". GUASCH PORTAS, V. y SOLER FUENSANTA, J.R. Cloud Computing, cláusulas contractuales y reglas corporativas vinculantes. *Revista de Derecho UNED.* 2014. nº 14. p. 247-269.

definiciones

detalles de la transferencia

- fundamentalmente categorías de datos

cláusula de tercero beneficiario

- para hacer exigible el clausulado por el interesado, aun no siendo parte, cuando sufra un daño como consecuencia del incumplimiento del contrato

obligaciones del exportador

- instrucciones para el tratamiento de los datos
- aseguramiento del cumplimiento de determinadas obligaciones por parte del importador
- interloución adecuada con responsable y con la AEPD en ámbitos como medidas de seguridad, modificación de legislación, acuerdos de subtratamiento...etc.

obligaciones del importador

- tratar los datos siguiendo las instrucciones
- medidas de seguridad técnicas y organizativas
- sistema de notificaciones
- ofrecer las instalaciones para auditorías de exportador y responsable
- obligaciones en referencia al subencargado

responsabilidad

- del exportador y, en caso de desaparición, asumidas por el importador y, en caso de desaparición de este, contra el subencargado ulterior por sus operciones de tratamiento

subtratamiento ulterior

- cadena de consentimiento y autorización.
- acuerdo por escrito
- responsabilidad del importador
- listado de acuerdos de subtratamiento a cargo del exportador/encargado

obligaciones tras el cese

- destrucción o devolución al exportador encargrado

Fuente: elaboración propia

Como subraya Cotino Hueso, “la ventaja para las empresas de servicios de nube españolas es que, si se logra la autorización de transferencia de datos siguiendo estas cláusulas

contractuales, no se precisa en general una ulterior si se mantiene lo establecido en el contrato"[769]. Solo tendrán que notificar —no pedir autorización— cada nueva transferencia internacional para que esta quede registrada. En la misma línea, el Grupo de Trabajo del artículo 29 elaboró con posterioridad, en 2014, un borrador de cláusulas ad hoc para este tipo de contratos[770], que sin embargo no vio la luz al no verse aprobada por la Comisión Europea.

1.3.4 Situación actual: modelos de cláusulas y potencial papel de las BCR

En definitiva, con esta fórmula, y como expone la propia Agencia Española de Protección de Datos, las garantías a aportar cuando el servicio de cloud computing implique una transferencia internacional de datos que necesite la autorización de la AEPD se puede canalizar o bien mediante un contrato entre el responsable y el encargado cuando este se encuentre radicado en un tercer país y con base en la Decisión de la Comisión de 2010 oportunamente modulado, o bien mediante un contrato entre el proveedor encargado y el subcontratado que actúa como subencargado y se encuentra radicado en un tercer país con base en el referido clausulado de 2012[771], sin perjuicio también de las necesarias matizaciones en su caso. La existencia de este último modelo de clausulado resulta de suma utilidad para la nube y evita la vorágine contractual a la que daría lugar la necesidad de suscribir un instrumento jurídico entre responsable y cada uno de los subencargados. Un buen ejemplo de su funcionalidad lo encontramos en la resolución adoptada por la autoridad danesa de protección de datos (Datatilsynet) denegando la posibilidad al ayuntamiento de Odense de almacenar los datos concernientes a las escuelas públicas en el servicio de "Google Apps". El Ayuntamiento señaló que los datos serían transferidos inicialmente a Google Ireland Limited; y Google posteriormente informó que mantiene todos sus datos en numerosos centros de datos en todo el mundo, incluyendo Estados Unidos y Europa, de tal modo que los datos inicialmente se compartirían con Irlanda y posteriormente entre Irlanda y potencialmente cualquier otro país en los que Google dispone de centros de dato. La

[769] COTINO HUESO, L. ob. cit. p. 99
[770] ARTICLE 29 DATA PROTECTION WORKING PARTY. Working document 01/2014 on Draft Ad hoc contractual clauses "EU data processor to non-EU sub-processor. 21 de marzo de 2014. Disponible en web: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp214_en.pdf
[771] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Consultas más frecuentes (FAQS). Garantías a aportar cuando el servicio de Cloud computing implique una transferencia internacional de datos que necesite la autorización de la AEPD. Disponible en web: http://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/detallePreguntaFAQ.jsf;jsessionid=8CA9474B37F14F146A661A74AE0EC25F?idPregunta=FAQ/00005

autoridad danesa señaló que los centros de datos en Estados Unidos estarían cubiertos por el Acuerdo de Puerto Seguro; sin embargo decidió asumir que los datos se transferirían no solo a Irlanda y Estados Unidos, sino también a otros países en los que Google dispusiera de centros de datos, incluyendo terceros países y consiguientemente la autoridad municipal incumpliría la legislación vigente ya que no tenía previsto –y aquí viene lo que más nos interesa– firmar ningún contrato basado en el clausulado estándar de la Comisión Europea con cada uno de los centros de datos de Google[772].

El hecho de que esto se contemplara dentro de un mismo Grupo Multinacional, nos lleva a las normas corporativas vinculantes como instrumento que podría ser utilizado para canalizar estas transferencias dentro del grupo, en este caso de Google, sin que por tanto resultara válido cuando quien interviniera fuera un proveedor o subencargado que no pertenezca a dicho Grupo. Hay que recordar que las denominadas BCR contemplan por un lado (WP 74, WP 107, WP 108, WP 133, WP 153, WP 154, WP 15) las transferencias internacionales de datos desde empresas del Grupo establecidas en la UE a empresas del Grupo fuera del UE, y pudiendo estas actuar como encargadas del tratamiento; pero también existen las BCR (WP 195, WP 195a y WP 204) que recogen las transferencias entre entidades del mismo Grupo que tratan los datos como encargados del tratamiento.[773] En este sentido, merece apuntarse otra de las soluciones, a día de hoy no contemplada, pero apuntada por Rubí Navarrete, que sería la adaptación de las BCR a un entorno desvinculado del grupo multinacional en el que el proveedor estableciera con carácter jurídicamente vinculante un marco de garantías y responsabilidades que deberá ser cumplido por el mismo y por cualquier entidad subcontratada[774].

Llama la atención sin embargo que la propia industria no haya visto esto como una opción. Así, en la propuesta de Código de Conducta[775] ya citada en numerosas ocasiones, se

[772] La descripción de este caso ha sido tomada de COCO CLOUD (CONFIDENCIALITY AND COMPLIANCE IN THE CLOUD). First Study of Legal and Regulatory Aspects of Cloud Computing. Version 1.0. 31 de octubre de 2014. 236 p. Disponible en web: http://www.coco-cloud.eu/sites/default/files/cococloud/files/content-files/deliverables/Coco_Deliverable%20D2.2_UO_20141031(1of2).pdf

[773] PRIETO HERGUETA, J. Transferencias internacionales de datos: las garantías de las normas corporativas vinculantes (BCR). *7ª Sesión Anual Abierta de la AEPD*. 21 de abril de 2015. Disponible en web: https://www.agpd.es/portalwebAGPD/jornadas/7_sesion_anual/common/JPH_TID_GARANTIAS_NORMAS_CORPORATIVAS_VINCULANTES_7SAA.pdf

[774] RUBI NAVARRETE, J. ob. cit. p. 105.

[775] C-SIG SUB-GROUP ON THE DATA PROTECTION CODE OF CONDUCT. Data Protection Code of Conduct for Cloud Service Providers Revised v1.0 22 June 2016. Disponible en web: https://ec.europa.eu/digital-single-market/en/news/data-protection-code-conduct-cloud-service-providers

contemplan por un lado las transferencias dentro del mismo Grupo a entidades que se encuentren en terceros países, bien sea bajo el paraguas de las BCR, de las cláusulas estandarizadas o bien porque concurren algunas de las excepciones previstas en el art. 26 de la Directiva 95/46. Por otro lado, se recogen los supuestos, de mayor trascendencia como acabamos de ver, en que no existe ese elemento corporativo, y consiguientemente solo se contempla la posibilidad de que la transferencia al subencargado en un tercer país tenga lugar bajo el modelo de clausulado aprobado por la Comisión –que cabe añadir en todo caso está previsto solo de responsable a encargado por lo que a nuestro juicio no es adecuado recogerlo aquí– o bien por algunas de las citadas excepciones contempladas en la Directiva.

A nuestro juicio la redacción del actual RGPD ayuda, y mucho, a la posibilidad apuntada por Rubí. Hasta ahora las BCR para los encargados de tratamiento únicamente se pueden realizar en el seno de un mismo Grupo multinacional. Sin embargo, y como se ha visto en el apartado correspondiente, la nueva regulación de las BCR puede dar entrada a esta posibilidad ya que se podría dar cabida a la prestación del servicio bajo el paraguas de "la unión de empresas dedicadas a una actividad económica conjunta" a la que hace referencia el art. 47.1 RGPD. A dicho interpretación ayuda también el hecho de que la Comisión Europea ya señalaba en el año 2013 la invitación a las autoridades nacionales de protección de datos a aprobar las normas corporativas vinculantes para los proveedores de servicios en la nube[776]. Atendiendo a las características de la subcontratación, que como decíamos están en el ADN de dicho tipo de servicios, parece razonable pensar que esta modulación podría ser posible. Es decir, a día de hoy, existe la posibilidad de que las BCR sean utilizadas intragrupo, es decir cuando el encargado y el subencargado pertenezcan al mismo Grupo. El RGPD creemos que puede estar abriendo la puerta a que se desvinculen del grupo corporativo multinacional y sean una vía más que adecuada para los prestadores de servicios en nube.

[776] COMISIÓN EUROPEA. 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. Disponible en web: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52012DC0529&from=ES

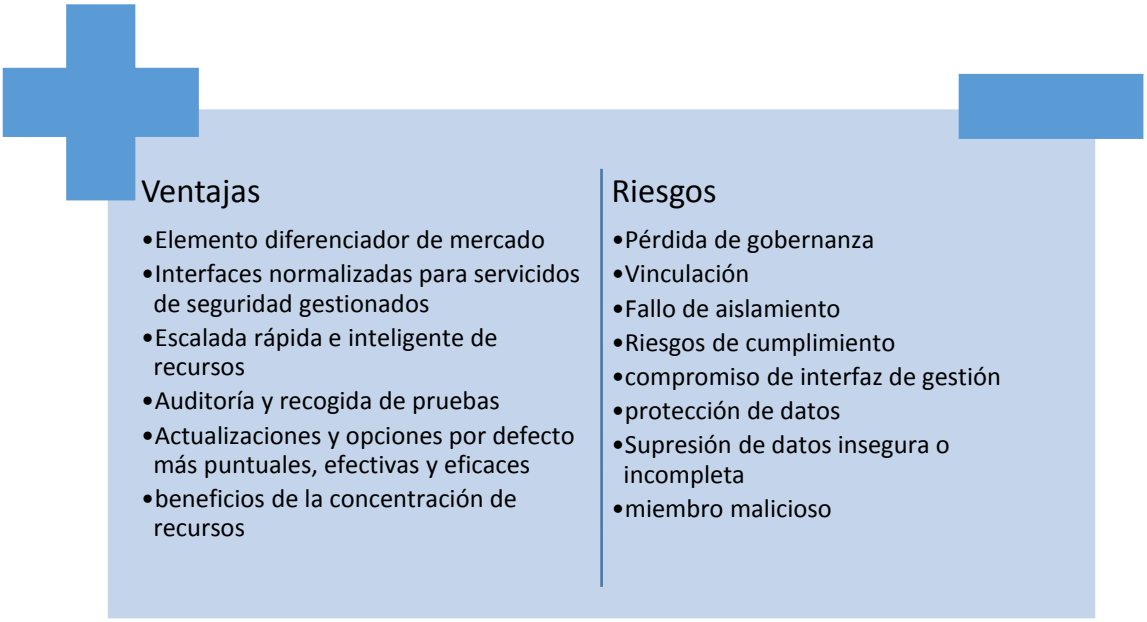
2 Las medidas de seguridad

2.1 Retos de la seguridad en la nube

Resulta paradójico que, por un lado, un gran proveedor nos pueda facilitar unas medidas de seguridad de naturaleza física y lógica que, salvo compañías especializadas, nadie puede garantizar en una infraestructura interna. Pero por otro lado, cualesquiera estudios o informes que se han realizado en el ámbito de la nube ponen de manifiesto que la seguridad, en términos de confidencialidad, disponibilidad e integridad de los datos, es una de las principales preocupaciones en la computación en nube. Esta paradoja de la seguridad en el entorno cloud viene claramente explicada por Cotino Hueso quien afirma que "Es cierto que —como se dijo— los servicios de la nube mejoran la seguridad y privacidad: la información no queda diluida en los numerosos usuarios responsables de ficheros no familiarizados con lo informático, la seguridad y la legalidad, sino concentrada en manos de especialistas en seguridad con grandes equipos, formación e infraestructura. No obstante, la información del usuario ya no queda localizada en la organización y bajo su control, sino que queda más o menos expuesta a terceros, ya por su acceso a la infraestructura de los prestadores de servicios de nube, ya por los riesgos de seguridad en las continuas conexiones entre el usuario y el prestador"[777]. Efectivamente estamos ante la cara y la cruz de una misma moneda. Por un lado, se cuenta con el respaldo y la solidez de empresas que tienen en la seguridad el pilar sobre el que se sostiene su negocio. En palabras de Serrera Cobos, es de esperar que un proveedor de servicios de cloud computing ponga todo su esfuerzo y experiencia al servicio de un entorno seguro, que constituye la base de su negocio[778]. Pero por otro, la confianza en las mismas tiene una naturaleza cuasi absoluta y se aleja del control del responsable la gestión de los datos y el cuidado de los mismos. Como dice Saiz Peña los clientes temen qué va a ocurrir con sus datos cundo salgan de su casa, si bien la realidad es que normalmente la seguridad implantada por los proveedores cloud es bastante superior a la que una empresa puede implantar por capacidad, conocimiento e inversión[779]. En fin, en otras latitudes, el profesor Nir Kshetri afirma que la nube es un arma de doble filo desde el

[777] COTINO HUESO, L. Algunas cuestiones clave de protección de datos en la nube: hacia una regulación nebulosa. p. 90.
[778] SERRERA COBOS, R. Cloud Computing y protección de datos. *Revista Dintel*. junio 2010. p. 182-184. Disponible en web: http://www.revistadintel.es/Revista/Numeros/Numero9/Normas/serrera.pdf
[779] SAIZ PEÑA, C.A. Medidas de seguridad en el *Cloud Computing;* en MARTINEZ MARTINEZ, R. (ed). *Derecho y cloud computing*. Thomson Reuters. Civitas. 2012. p. 149-178.

punto de vista de la seguridad[780]. Esta dualidad también la han recogido entornos oficiales. Así, por ejemplo, la ENISA ha puesto de manifiesto estas dos vertientes, tal y como quedan reflejadas en la siguiente figura:



Fuente: elaboración propia

A estas reflexiones cabe añadir los pronunciamientos oficiales, incluso en el plano normativo, y basta para ello observar la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (conocida coloquialmente como Directiva NIS). En esta se observan particulares referencias a la nube, por ejemplo apelando a que las administraciones públicas que utilizan este tipo de servicios puedan considerar conveniente exigir a los proveedores medidas de seguridad adicionales mediante obligaciones contractuales, más estrictas más allá de las exigidas por la Directiva (Considerando 54); y reiterando que la Directiva no debe ser óbice para que los Estados adopten medidas nacionales que obliguen a los organismos del sector público a garantizar unas condiciones de seguridad específicas cuando contraten servicios de computación en nube (Considerando 56).

[780] KSHETRI, N. Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Journal Telecommunications Policy archive*. mayo de 2013. Vol. 37. p. 372 a 386.

Cabe decir en todo caso que incidentes de seguridad en cualquier desarrollo tecnológico han existido siempre, y el entorno cloud, y algunos de sus máximos exponentes, no han sido ajenos[781]. De hecho, como apunta el profesor Jaydip Sen, existen en este entorno dos tipos de amenazas a la seguridad: aquella que surge directamente de la tecnología de cloud y aquellos que son nuevos vectores a problemas de seguridad ya existentes[782].

En Estados Unidos, y como se observa en la siguiente figura, el NIST ha señalado los siguientes aspectos clave de seguridad en la nube:

[781] Varios ejemplos en CHEN, D. y ZHAO, H. Data Security and Privacy Protection Issues in Cloud Computing, *2012 International Conference on Computer Science and Electronics Engineering*. 2012. Vol. 1. p. 647-651.

[782] SEN, J. Security and Privacy Issues in Cloud Computing. *Architectures and Protocols for Secure Information Technology Infrastructures*. 2013. p. 1-42. Disponible en web: https://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf

Gobernanza
Cumplimiento
•Ubicación de los datos •Investigación electrónica
Confianza
•Acceso desde dentro •Propiedad de los datos •Servicios complejos •Visibilidad •Gestión de los riesgos
Arquitectura
•Superficie de ataque •Protección de la red virtual •Datos auxiliares •Protección del cliente •Protección del servidor
Identidad y control de acceso
•Autenticación •Control de acceso
Aislamiento de software
•Complejidad del hipervisor •Vectores de ataque
Protección de datos
•Aislamiento •Saneamiento
Disponibilidad
•Fallos temporales •Fallos prolongados o permanentes •Denegación de servicio •Valor concentrado
Respuesta a indidentes

Fuente: elaboración propia con base en información del NIST

En el plano doctrinal, los profesores Chen y Zhao[783], afirman que, debido a las características de escalabilidad dinámica, abstracción del servicio, y transparencia en la localización, todos los tipos de aplicaciones y datos de una plataforma cloud no tienen infraestructura fija ni fronteras de seguridad. Y añaden cuatro ejemplos que reflejan la particular problemática del

[783] Ver nota anterior.

entorno cloud para la seguridad: en caso de una quiebra en la seguridad, resulta difícil aislar un recurso físico particular que haya sido amenazado o comprometido; de acuerdo con los modelos de prestación del servicio, los recursos pueden ser propiedad de múltiples proveedores, lo que dificulta implantar unas medidas de seguridad unificadas; debido a la apertura de la nube y a la compartición de recursos virtualizados por múltiples usuarios, los datos del usuario pueden ser objeto de acceso por otros usuarios no autorizados; debido a que la plataforma cloud tiene que lidiar con almacenamiento masivo de información y facilitar un acceso rápido, las medidas de seguridad tienen que ajustarse a la necesidad del tratamiento masivo de información.

Por su parte, para el referido Jaydip Sen, y tal y como se describe en la figura, existen seis áreas específicas en el entorno cloud en las que el equipamiento y el software requieren una atención de seguridad substancial: la seguridad de los datos en reposo, la seguridad de los datos en tránsito, la autenticación de los usuarios/aplicaciones/procesos, una robusta separación entre los datos que pertenecen a diferentes clientes, los aspectos legales y regulatorios y las respuestas a los incidentes.

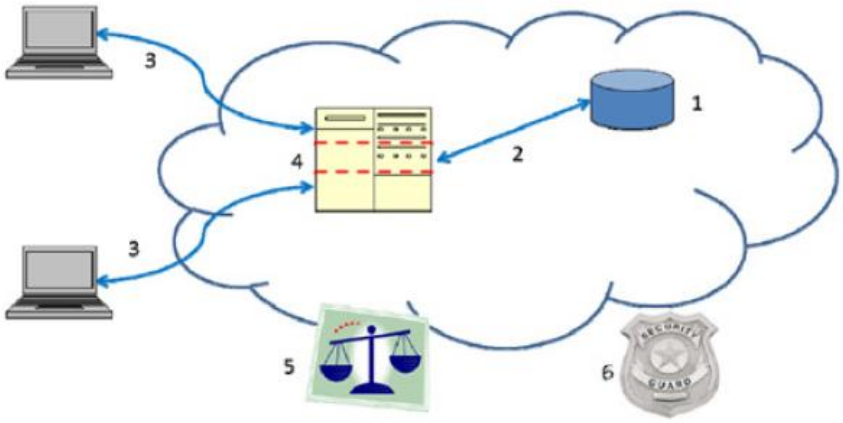
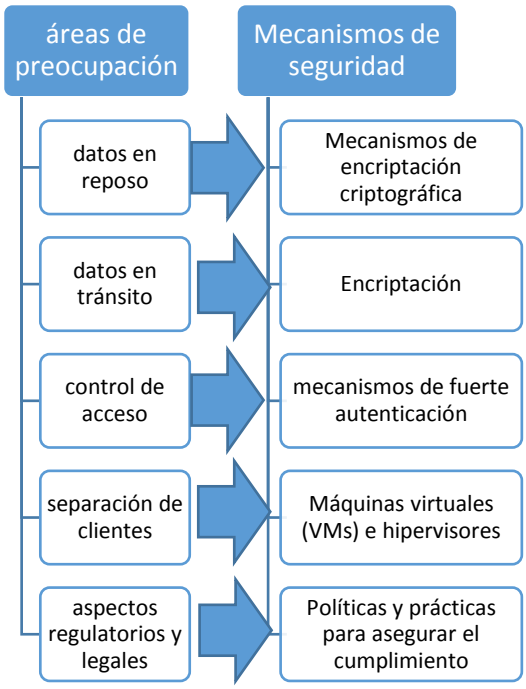


Figure 2: Areas for security concerns in cloud computing: (1) data at rest, (2) data in transit, (3) authentication, (4) separation between customers, (5) cloud legal and regulatory issues and (6) incident response.

Fuente: *Security and Security and Privacy Issues in Cloud Computing.*

Este mismo autor señala cuáles son las mejores tecnologías para el aseguramiento de cada una de esas potenciales vulnerabilidades



Fuente: elaboración propia con base en el artículo mencionado en el gráfico anterior

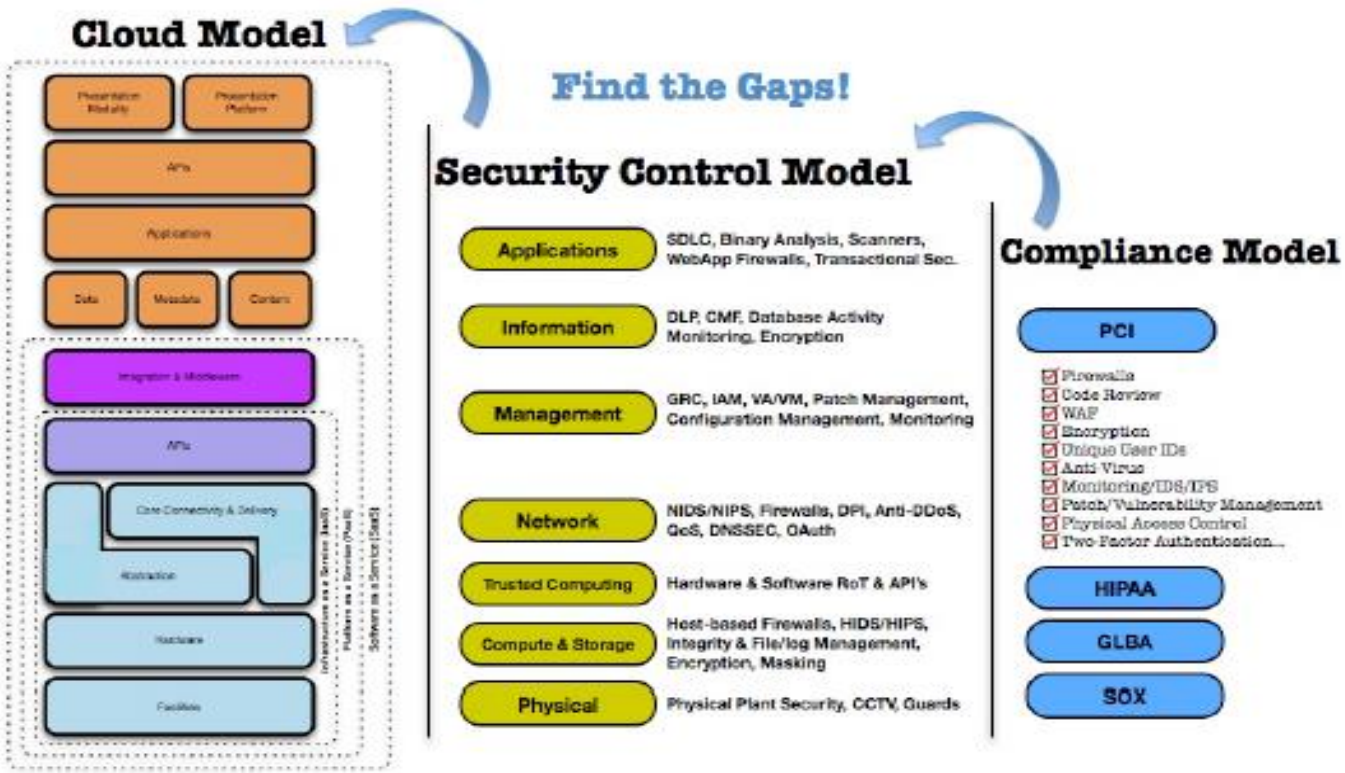
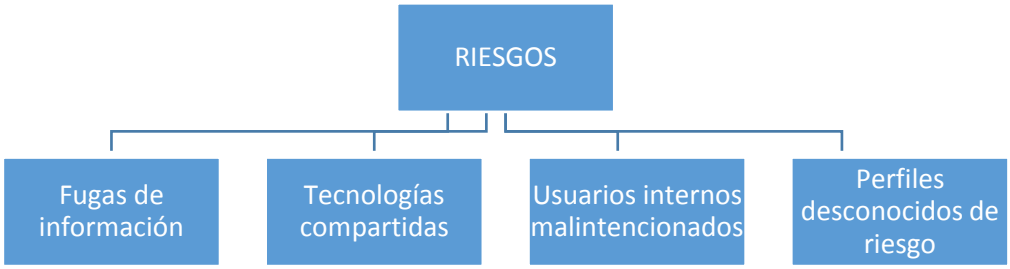


Figure 5—Mapping the Cloud Model to the Security Control & Compliance

Fuente: *CSA. Seucirty Guidance for Critical Areas of Focus in Cloud Computing 3.0*

En nuestro país, también es unánime la posición a la hora de subrayar los riesgos en materia de seguridad fruto de la evolución tecnológica. Así, Serrera Cobos señala que "*Cloud computing* es la evolución del *outsourcing* tradicional, con ventajas ¡y riesgos! adicionales sobre todo en seguridad". González y Rilo subrayan que "La nueva situación genera nuevos riesgos y son necesarias, por tanto, nuevas medidas de seguridad en aspectos técnicos, legales y organizativos, ya que el modelo actual de seguridad carece, en la mayoría de las ocasiones, de la eficiencia y efectividad necesarias en este nuevo modelo de computación"[784]. Son estos mismos autores quienes, señalan los siguientes riesgos de manera resumida[785]:



Fuente: elaboración propia

También la industria ha señalado cuáles son las principales amenazas a la seguridad y basta para ello ver las dos figuras siguientes[786]:

[784] GONZÁLEZ, D. y RILO, J. *Cloud Computing* y seguridad. *XII Reunión Española sobre Criptología y Seguridad de la Información (RECSI 2012).* 2012. Disponible en web: http://recsi2012.mondragon.edu/es/programa/recsi2012_submission_35.pdf
[785] *Idem.*
[786] Ambas han sido extraídas del informe elaborado por el antiguo INTECO. Riesgos y amenazas en Cloud Computing. Ministerio de Industria, Turismo y Comercio. marzo de 2011. Disponible en web: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf

Fuente: elaboración propia con base en la información de *Cloud Security Alliance*

Fuente: elaboración propia con base en la información de *Gartner*

En fin, en el plano de la industria, la figura que se recoge a continuación contempla también un resumen adecuado de los principales riesgos para la seguridad.

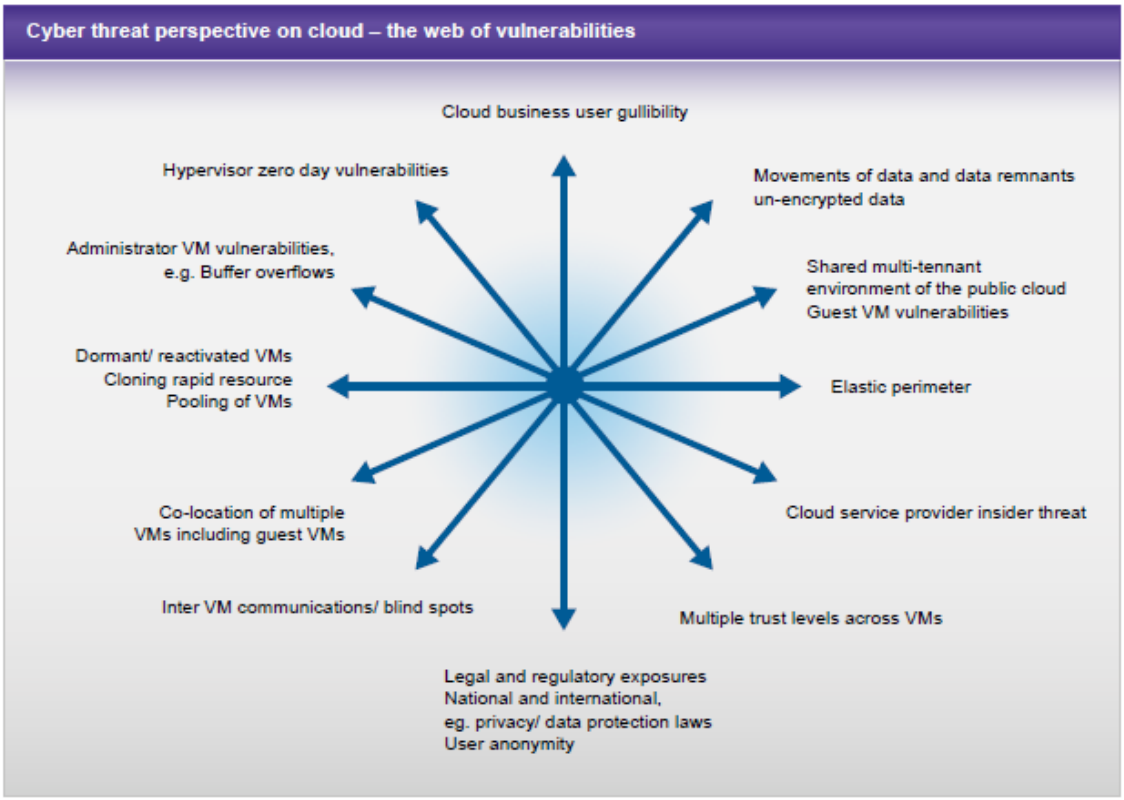


Figure 1-2 – Cloud vulnerabilities

Fuente: *BT cloud Compute Security*

2.2 El tratamiento jurídico de la seguridad: nivel de riesgo vs. nivel de seguridad

Pero al margen de los nuevos retos tecnológicos que industria y doctrina han subrayado reiteradamente, y que sin duda tienen una gran importancia, siguiendo a Marzo Portera, podemos decir que no es un problema de seguridad técnica -en gran medida por la asimetría de medios e información, nos permitimos añadir- lo que dificulta las relaciones entre los diversos actores que operan en las relaciones de *cloud computing*, sino un problema de seguridad legal[787]. Y esta afirmación se confirma si se observa, sin temor a equivocarse, que las medidas de seguridad de los datos han constituido siempre uno de los vectores que informan la normativa de protección de datos

[787] MARZO PORTERA, A. Privacidad y cloud computing, hacia dónde camina Europa. Ob. cit. p. 226.

Así, ya el art. 7 del Convenio 108 del Consejo de Europa establece que "Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados". De manera más extensa, la Directiva 95/46 contempla una serie de mandatos claros a los Estados miembros en su artículo 17 y que se concretan en: establecer la obligación del responsable de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra 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, y contra cualquier otro tratamiento ilícito de datos personales; en la obligación del responsable, en nuestro caso el cliente, de elegir un encargado, el proveedor, que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumple dichas medidas..

Sin entrar en mayores detalles por cuanto se desarrollará a lo largo del presente apartado, el RGPD tiene en la seguridad un vector informador de todo el texto y basta para ello observar algunos de sus Considerandos introductorios[788]. Es en concreto la Sección 2 del Capítulo IV la que lleva por rúbrica "Seguridad de los datos personales", aunque como mencionaremos,

[788] Se habla así de que "Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento" (Considerando 39); Para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento (Considerando 81); A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales (Considerando 83); tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas (Considerando 85); El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias (Considerando 86).

existen muchos otros aspectos no recogidos en dicha Sección, que se encuentran estrechamente vinculados y son verdaderas proyecciones del principio de seguridad de los datos.

En el ámbito nacional, el art. 9 LOPD recoge la seguridad de los datos, siguiendo el referido mandato de la Directiva y remitiéndose al ROPD en cuanto a los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de datos. Es precisamente el ROPD el que en su Título VIII lleva a cabo una regulación sumamente detallada de las medidas de seguridad. También la LOPD, en su artículo 44.2 h), dispone que constituirá infracción grave de la Ley "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".

Las continuas llamadas a las medidas de seguridad, no son únicamente propias de nuestro entorno geográfico y sirva para ello atender a la normativa estadounidense. Basta observar en el ámbito sanitario la HIPAA[789] o en el financiero la Ley Gramm-Leach-Bliley[790]. Ambas por cierto imponen severas restricciones a la hora de llevar los datos a la nube, en gran medida por la particular naturaleza de los mismos.

En clara conexión con la vertiente normativa, las autoridades de protección de datos de diferentes países han puesto de manifiesto su preocupación por todo lo relacionado con la seguridad de los datos. La autoridad británica ha señalado que una parte importante a la hora de elegir el proveedor de servicios adecuado es una evaluación de la seguridad que tiene implantada. Y añade que es importante recordar que la seguridad no es solamente un factor a tener en cuenta, sino uno muy importante[791]. Sin perjuicio de otras consideraciones, en las que se ponen de manifiesto los riesgos vinculados a la seguridad de los datos, la autoridad francesa -volviendo a la idea de las dos caras de la misma moneda antes apuntada- reconoce que las ofertas de servicios en nube pueden tener unos niveles de seguridad más altos que aquellos que pueden ser garantizados por las PYMES[792]. En fin, en España, cabe recordar la muy detallada Guía de Seguridad de Datos que elaboró nuestra

[789] *Health Insurance Portability and Accountability Act.* El acceso al texto oficial de la norma en el siguiente enlace: https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm
[790] El nombre oficial es *Financial Services Modernization Act*. El acceso al texto oficial de la norma en el siguiente enlace: https://www.gpo.gov/fdsys/pkg/STATUTE-113/pdf/STATUTE-113-Pg1338.pdf
[791] INFORMATION COMMISSIONER'S OFFICE. Guidance on the use of cloud computing. Ob. Cit. p. 13.
[792] COMMISSION NATIONAL DE L'INFORMATIQUE ET DES LIBERTÉS. Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing. ob. Cit. p. 1,

Agencia en 2010 y a la que luego nos referiremos[793]; y con menor detalle también dispone de una guía la autoridad irlandesa[794].

El Grupo de Trabajo del artículo 29 por su parte ha tratado el tema de la seguridad en muy diferentes dictámenes, aunque siempre al hilo del tratamiento de otras cuestiones, ratificándose así, como hemos apuntado, el carácter transversal de esta materia y su vinculación a cualquier desarrollo o derivada tecnológicos. A título de ejemplo podemos observar su pronunciamiento específico sobre Cloud Computing al que luego nos referiremos, su preocupación respecto a las implicaciones en dicha cuestión de la Internet de las Cosas (IoT)[795], o su reciente pronunciamiento con motivo de la revisión de la Directiva sobre la privacidad y las comunicaciones electrónicas[796]

También con proyección normativa, como no podía ser de otro modo, desde la industria, el Código de Conducta para los Proveedores de Servicios Cloud trata esta materia. En concreto el Anexo B de la versión actualmente existente recoge los objetivos de seguridad. Su finalidad es definir un conjunto mínimo de objetivos de seguridad de la información que deben ser alcanzados por un proveedor de servicios: Dirección de gestión para la seguridad de la información, organización de la seguridad de la información, seguridad de los recursos humanos, gestión de activos, controles de acceso, criptografía, seguridad física y del entorno, seguridad operacional, seguridad de las comunicaciones, desarrollo del sistema y mantenimiento, proveedores, gestión de incidentes y seguridad de la información en la continuidad de negocio.

Centrándonos ya en la normativa europea, ya hemos señalado anteriormente la importancia que el RGPD da a la seguridad en sí misma y a las medidas de seguridad como proyección.

---

[793] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía de Seguridad de Datos. 2010. Disponible en web: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_SEGURIDAD_2010.pdf

[794] DATA PROTECTION COMMISSIONER. Data Security Guidance. Disponible en web: https://www.dataprotection.ie/docs/Data-security-guidance/1091.htm#19

[795] ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 8/2014 on the on Recent Developments on the Internet of Things. 16 de septiembre de 2014. Disponible en web: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[796] 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). El Grupo de trabajo se ha pronunciado sobre su reforma. Así, ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC). 19 de julio de 2016. Disponible en web: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf

Así se manifiesta en el hecho de que la seguridad se incluya entre los principios del tratamiento. En concreto el art. 5 RGPD establece los principios de integridad y confidencialidad al afirmar que los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

A pesar de las numerosas definiciones que se recogen en su artículo 4, el RGPD no nos da una definición de qué debemos entender por medidas de seguridad. Lo más cercano que nos encontramos es el apartado 12 en el que se define la "violación de la seguridad de los datos personales" como toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. El artículo 3.g) de la Decisión de la Comisión de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, las define como: "las destinadas a proteger los datos personales contra su destrucción accidental o ilícita o su pérdida accidental, su alteración, divulgación o acceso no autorizados, especialmente cuando el tratamiento suponga la transmisión de los datos por redes, o cualquier otra forma ilícita de tratamiento".

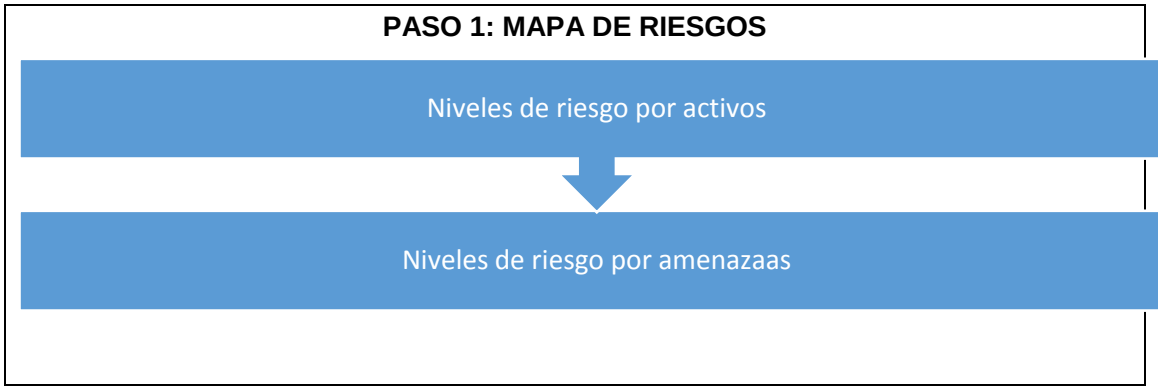
Forma parte de este mismo espíritu vertebrador de la seguridad el de la privacidad por diseño y por defecto[797] (art. 25 RGPD), que constituye una de sus grandes novedades; el registro de las actividades de tratamiento, y más concretamente que el mismo incluya una descripción general de las medidas técnicas y organizativas de seguridad tanto por parte del cliente responsable (art. 30.1.g) como por parte del encargado proveedor (art. 30.2.d), aunque cabe subrayar que en ambos supuestos las obligaciones solo se aplican a empresas que empleen a, al menos, 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos o relativos a condenas e infracciones penales (art. 30.5 RGPD). Llama la atención en este sentido que el RGPD, desarrollado con la finalidad de proteger un derecho fundamental como el derecho a la protección de los datos personales, base la articulación de garantías organizativas y tecnológicas, pero también jurídicas, en la dimensión de la

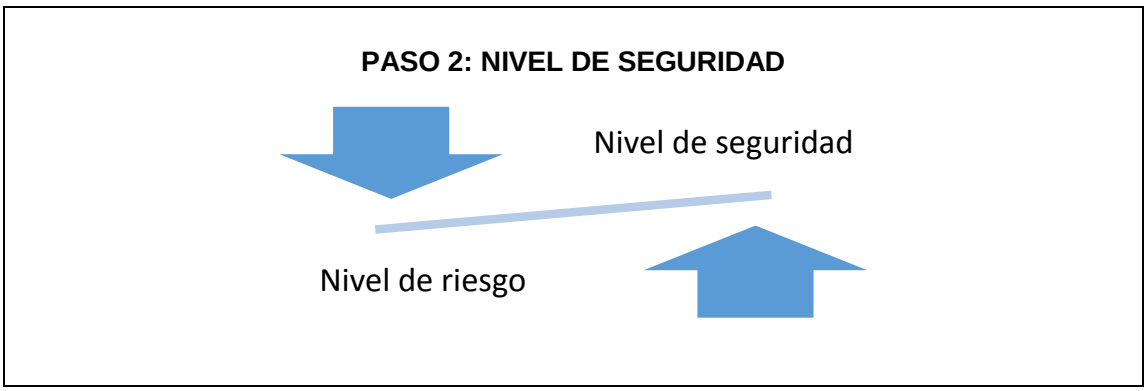
[797] Para un estudio con detalle, ver VILLARINO MARZO, J. Privacidad desde el diseño en la propuesta de reglamento europeo de protección de datos. *Revista Aranzadi de derecho y nuevas tecnologías*, ISSN 1696-0351. 2013. Nº. 32. p. 45-68

organización. Parece razonable que así lo sea cuando se cumpla la segunda condición, es decir, que la actividad pueda entrañar un riesgo para los derechos y libertades de los interesados, y que no esté condicionado sin embargo a una mera cuestión numérica, máxime si pensamos en las enormes diferencias de tejido empresarial que existen entre algunos países de la Unión Europea.

En cuanto al tratamiento que lleva a cabo de la seguridad propiamente dicha, el RGPD obliga a responsable y encargado (art. 32.1.a)) a aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que incluya entre otros: la seudonimización y el cifrado de datos, la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico; y un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

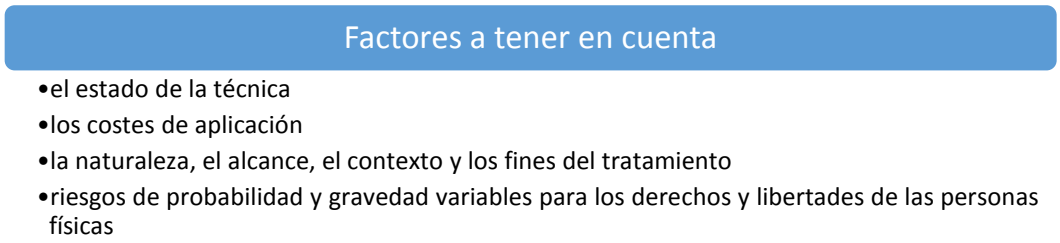
La clave del párrafo anterior viene dada precisamente por la necesidad de que el nivel de seguridad se compadezca con el nivel de riesgo. Este constituye el principio fundamental que informa la normativa de seguridad. Para ello es necesario lógicamente, como refleja la figura, realizar un mapa de riesgos y ajustar el nivel de seguridad a las conclusiones de dicho mapa.





Fuente: elaboración propia

Esta idea o proceso lo recoge la propia norma de manera indirecta. En concreto, el apartado 2 del artículo 32 RGPD señala que, al evaluar que el referido equilibrio o adecuación existe, se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. A mayor abundamiento, el apartado 1 señala la necesidad de atender a los siguientes factores a la hora de adoptar las medidas técnicas y organizativas para garantizar el nivel de seguridad adecuado:



Fuente: elaboración propia

La idea fuerza que subyace por tanto a las obligaciones del cliente en cuanto que responsable y del proveedor de servicios en nube en cuanto encargado, es la necesidad de que el nivel de seguridad se adecúe al nivel de riesgo. Por tanto, nos encontramos con unos niveles de seguridad variables y que no son fijados a priori por el RGPD.

En la misma línea se sitúa la denominada “Evaluación de impacto relativa a la protección de datos” que está focalizada en los supuestos en que el nivel de riesgo sea alto. A pesar de que no hay un listado cerrado, el propio RGPD nos da unos supuestos indicativos de cuándo se tiene que llevar a cabo: evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; tratamiento a gran escala de las categorías especiales de datos a, o de los datos relativos a condenas e infracciones penales, o la observación sistemática a gran escala de una zona de acceso público.

En todo caso, y por si los mencionados supuestos no son suficientes, hay un llamamiento a las autoridades de protección de datos para que elaboren un listado en el que se incluyan los tipos de operaciones que exigen esa evaluación y aquellas otras que no lo exigen, y, por ende, añadimos, aquellas que se considera que implican un riesgo alto y aquellas otras que no. En este punto cabe reseñar que la AEPD elaboró en octubre de 2014 en una “Guía para una Evaluación de Impacto en la de Protección Datos Personales”[798] el referido listado, si

[798] En concreto se trata de: cuando se enriquezca la información existente sobre las personas mediante la recogida de nuevas categorías de datos o se usen las existentes con nuevas finalidades o en formas que antes no se usaban, en particular, si los nuevos usos o finalidades son más intrusivos o inesperados para los afectados; cuando se lleve a cabo un tratamiento significativo no incidental de datos de menores o dirigido especialmente a tratar datos de estos, en particular si tienen menos de catorce años; cuando se vaya a llevar a cabo un tratamiento destinado a evaluar o predecir aspectos personales relevantes de los afectados, su comportamiento, su encuadramiento en perfiles determinados (para cualquier finalidad), encaminado a tomar medidas que produzcan efectos jurídicos que los atañen o los afectan significativamente y, en particular, cuando establezcan diferencias de trato o trato discriminatorio o que puedan afectar a su dignidad o su integridad personal; cuando se traten grandes volúmenes de datos personales a través de tecnologías como la de datos masivos (Big data), internet de las cosas (Internet of Things) o el desarrollo y la construcción de ciudades inteligentes (smart cities); cuando se vayan a utilizar tecnologías que se consideran especialmente invasivas con la privacidad como la videovigilancia a gran escala, la utilización de aeronaves no tripuladas (drones), la vigilancia electrónica, la minería de datos, la biometría, las técnicas genéticas, la geolocalización, o la utilización de etiquetas de radiofrecuencia o RFID; cuando el tratamiento afecte a un número elevado de personas o, alternativa o adicionalmente, se produzca la acumulación de gran cantidad de datos respecto de los interesados; cuando se cedan o comuniquen los datos personales a terceros y, en particular, siempre que se pongan en marcha nuevas iniciativas que supongan compartir datos personales con terceros que antes no tenían acceso a ellos, ya sea entregándolos, recibiéndolos o poniéndolos en común de cualquier forma; cuando se vayan a transferir los datos a países que no forman parte del Espacio Económico Europeo (EEE) y que no hayan sido objeto de una declaración de adecuación por parte de la Comisión Europea o de la Agencia Española de Protección de Datos; cuando se vayan a utilizar formas de contactar con las personas afectadas que se podrían considerar especialmente intrusivas; cuando se vayan a utilizar datos personales no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica; o cuando la recogida tenga como finalidad el tratamiento sistemático y masivo de datos especialmente protegidos. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía para una Evaluación de Impacto en la de Protección Datos Personales. 31 de octubre de 2014. Disponible en web: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

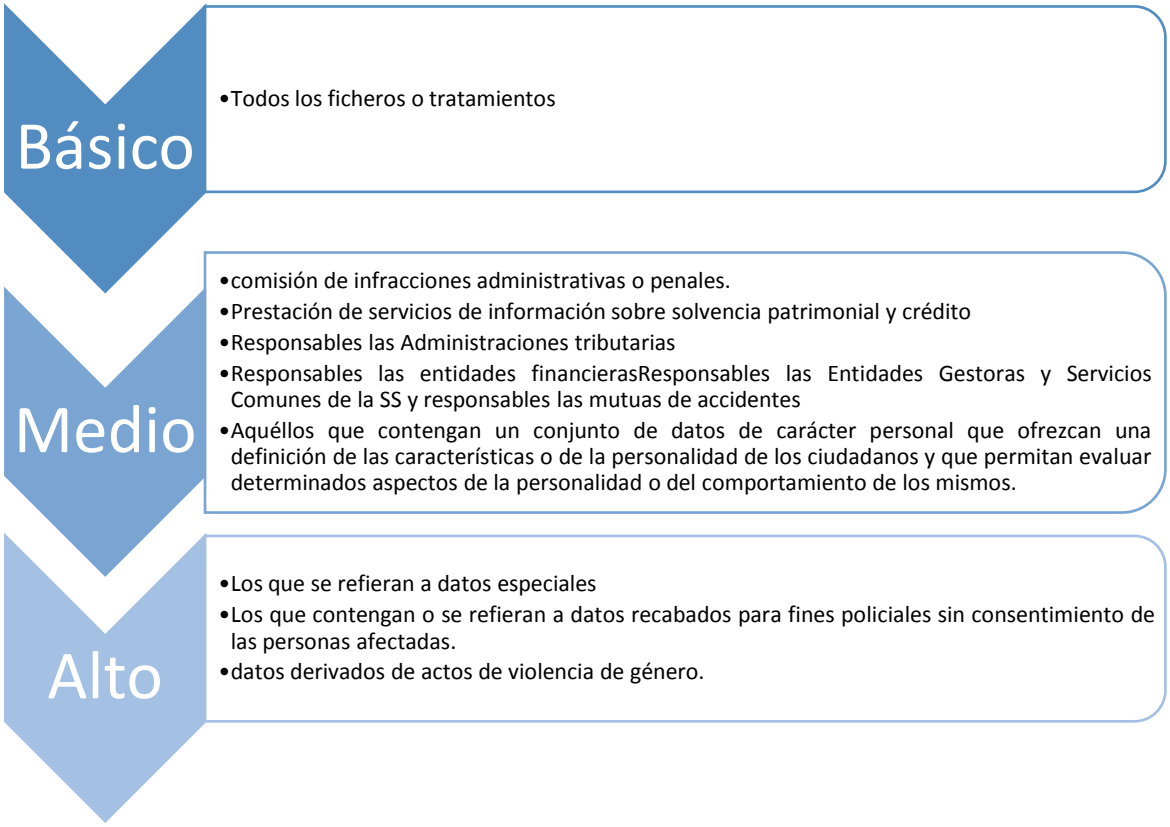
bien lo hizo aclarando que en estos casos era aconsejable y que se trataba de una enumeración indicativa.

De particular relevancia para la materia que nos ocupa es el supuesto que añade la propia AEPD: la existencia de riesgos específicos de seguridad que puedan comprometer la confidencialidad, la integridad o la disponibilidad de los datos personales y, especialmente, y aquí es donde entra en consideración la naturaleza remota de la computación en nube, si estas situaciones de riesgo se producen cuando los datos circulan o se accede a ellos a través de redes de telecomunicaciones.

Cabe subrayar desde el punto de vista de los sujetos obligados que, si bien es cierto que la obligación de seguridad, como ya se ha dicho, iría dirigida tanto al proveedor como al cliente, en el caso de la Evaluación de Impacto se dirige exclusivamente al cliente.

Hemos visto que el RGPD nos habla exclusivamente de un nivel de riesgo alto, en cuanto que vinculado a la evaluación y la conexión indirecta que se puede dar con los supuestos que acabamos de enumerar. En referencia a los niveles de riesgo, cabe recordar que en la actualidad la Directiva no fija dichos niveles, y la LOPD se limita a realizar su división en el artículo 20.h) o 26, pero sí los describe y detalla el ROPD. La propia Exposición de Motivos de este afirma que "…el reglamento trata de ser particularmente riguroso en la atribución de los niveles de seguridad, en la fijación de las medidas que corresponda adoptar en cada caso y en la revisión de las mismas cuando ello resulte necesario". En concreto distingue[799]:

[799] La triple dicotomía de la gestión de riesgos se contemplaba ya en el viejo 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.



Fuente: elaboración propia con base en el art. 81 ROPD

Como una apreciación previa, cabe subrayar una variación de lo previsto en el RGPD con respecto a la categorización del ROPD. Este último está basado, a la hora de situar el nivel de riesgo como alto, en la naturaleza de los datos tratados. En el año 2010, en su Guía sobre la Seguridad de Datos, la Agencia decía que la clasificación de los niveles de riesgo se realiza atendiendo a la naturaleza de la información tratada, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información. Con el nuevo enfoque del RGPD y también de la propia Guía de la Agencia del año 2014, no se está atendiendo tanto a la naturaleza de los datos tratados, que también (por ejemplo, los menores), cuanto a otros aspectos tales como la tecnología utilizada (sin referencia alguna al cloud computing como hemos visto) o el volumen de datos. Esto mismo se observa si se hace una comparativa de los textos: y es que la Directiva 95/46, en su artículo 17.1, habla de que las medidas de seguridad se adoptan teniendo en cuenta de los conocimientos técnicos existentes y del coste de su aplicación, para garantizar un nivel de seguridad apropiado en relación con *los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse*; mientras que el referido artículo 32, teniendo en cuenta la

adecuación al riesgo, señala, como hemos ya transcrito, que las medidas de seguridad se adaptan teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas. Por tanto, no se hace una especial mención a la categoría o al tipo de datos que están siendo objeto de tratamiento. De hecho, se utilizan unos conceptos que resultan en cierta medida indeterminados y que adquieren virtualidad en el entorno del *cloud computing*. Al respecto nos arroja algo de luz Saiz Peña, quien lo hace con base en los términos utilizados por el actual artículo 17 de la Directiva 95/46. Así, cuando se habla del estado de la técnica, y en un entorno como el cloud, se está refiriendo a sistemas de protección dinámicos, escalables, flexibles y adecuados a los avances tecnológicos, sin que sea lógico el establecimiento de medidas muy específicas y concretas que puedan quedar obsoletas. Cuando se habla del coste de aplicación, el citado autor sostiene que los estudios de las compañías de *research* y *benchmarking* de reputación mundial definen muy bien la evolución de las inversiones en seguridad y pueden ser un criterio orientativo a tener en cuenta en la aplicación de las medidas de seguridad. Por último, en lo concerniente a los riesgos que presenta el tratamiento, se limita a apuntar la importancia de realizar un análisis de riesgos de la información y su correspondiente gestión[800].

La adecuación de las medidas de seguridad al nivel de riesgo, aunque este se concrete como hemos visto de manera diferente, es por tanto el esquema que hoy informa ya la aplicación de unas u otras medidas de seguridad y que, como hemos anunciado se encuentran desarrolladas en el ROPD, de manera acumulativa, en los artículos 89 a 94 (nivel básico), 95 a 100 (nivel medio), y 101 a 104 (nivel alto). Entre las mismas se tratan cuestiones como el responsable de seguridad, el personal, las incidencias, control de acceso, identificación y autenticación, gestión de soportes, copias de respaldo, criterios de archivo, almacenamiento, custodia de soportes, copias o reproducciones, auditorías, telecomunicaciones o traslado de la información.

[800] SAIZ PEÑA, C.A. Medidas de seguridad en el *Cloud Computing,* Ob. cit. p. 160 a 163.

2.3 Algunos aspectos particularmente relevantes para la nube

2.3.1 Las comunicaciones, documentación y protocolos

Vamos a centrarnos en aquellos aspectos de seguridad que pueden tener un mayor impacto en la tecnología *cloud.* En este sentido, resulta relevante en el campo concreto del cloud computing, la actual redacción del art 85 ROPD concerniente al acceso a datos a través de redes de comunicaciones y en el que se subraya que las medidas de seguridad exigibles, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local. En esta línea se pronuncia también la AEPD en su Guía[801]. En el plano doctrinal, Javier Puyol hace especial hincapié en esta cuestión al recordar la importancia que cobran en este sistema las líneas de comunicaciones que, obviamente, han de ser seguras[802].

Especial relevancia tiene también el denominado documento de seguridad, al que no se hace mención ni en la Directiva ni en el RGPD, pero sí en el ROPD, cuyo art. 88 señala que recogerá las medidas de índole técnica y organizativa que serán de obligado cumplimiento para el personal con acceso a los sistemas de información. Sin perjuicio de la concreción una vez se implante el RGPD, actualmente recoge unos contenidos mínimos: ámbito de aplicación con especificación detallada de los recursos protegidos; medidas, normas, procedimientos, reglas y estándares de seguridad; funciones y obligaciones del personal, estructura y descripción de los ficheros y sistemas de información; procedimiento de notificación, gestión y respuesta ante incidencias; procedimiento de copias de respaldo y recuperación de datos; medidas adoptadas en el transporte, destrucción y/o reutilización de soportes y documentos. A ello se sumará la identificación del responsable de seguridad y el control periódico del cumplimiento del documento. Además, en el caso que nos ocupa, el cliente deberá hacer constar que ha contratado unos servicios cloud, con referencia al contrato y a su periodo de vigencia, así como los ficheros sometidos a este contrato, pudiendo delegar la llevanza del documento en el propio proveedor cloud siempre que este preste el servicio en la totalidad o parte de los ficheros y tratamiento de los datos (artículo 88.6 ROPD). A ello se añadirá lo previsto en el actual artículo 82.2 ROPD que recoge que si el servicio fuera prestado por el encargado/proveedor en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del

[801] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía para clientes que contraten servicios de Computing. ob. cit. p. 16.
[802] PUYOL MONTERO, J. Algunas consideraciones sobre *Cloud Computing*. ob. cit. p. 207.

mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

La importancia de la seguridad tiene también su manifestación en la necesaria articulación o protocolización de mecanismos que mitiguen los daños que se puedan derivar de las inevitables quiebras o incidencias en aquella. Resulta imposible humana, técnica y legalmente reducir el riesgo a cero, tal y como se ha demostrado al comienzo de este apartado. Es por ello que desde el punto de vista normativo se fijan una serie de criterios que contribuyan a una conducta responsable por parte del cliente y del proveedor en salvaguarda tanto de su propia labor y negocio, como en último lugar, de los terceros titulares de los datos que se puedan ver comprometidos.

En este sentido, ya 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 (modificada por la Directiva 2009/136/CE), tras recordar que una violación de los datos personales puede causar, si no se toman medidas de manera rápida y adecuada, pérdidas económicas sustanciales y perjuicios sociales para el particular afectado, incluida la usurpación de la identidad; recoge, en su ámbito específico, que, tan pronto como el proveedor de servicios de comunicaciones electrónicas disponibles al público se percate de que se ha producido una violación de la seguridad, debe notificarla a la autoridad nacional competente. Y añade que los abonados o particulares cuyos datos e intimidad puedan verse afectados negativamente por dichas violaciones deben recibir notificación inmediata para que puedan adoptar las precauciones necesarias

2.3.2 Incidencias de seguridad y protocolos de notificación

La normativa actual en España contempla una serie de actuaciones referidas a las incidencias de seguridad, que por cierto son definidas por la Agencia, con carácter no exhaustivo, como cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como cualquier anomalía que afecte o pueda afectar a la seguridad de los datos. En concreto, ya desde las medidas de seguridad de carácter básico, el artículo 90 ROPD contempla la obligación de un procedimiento de notificación y gestión de las incidencias que afecten a los datos y el establecimiento de un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido o detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas. En definitiva, se fija un protocolo de actuación.

En el caso del nivel de seguridad medio, se añade la necesidad de incorporar al registro de incidencias, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación. Por último, mencionar que en el nivel alto de seguridad hay que incorporar, en el campo de la recuperación de la información, la conservación de una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan.

Como resulta lógico, el RGPD ha incidido también en los mecanismos de notificación de las quiebras de la seguridad, siguiendo más la línea de la referida Directiva 2002/58, y prueba de ello es el considerando 59 de la Directiva 2009/136 en el que se afirmaba que "Este interés de los usuarios por ser informados no se limita, obviamente, al sector de las comunicaciones electrónicas, por lo que deben introducirse, a escala comunitaria y con carácter prioritario, requisitos de notificación explícitos y obligatorios en todos los sectores".

En el entorno cloud, y conforme al art. 33 RGPD, será el cliente quien lo deba notificar a la autoridad de control sin "dilación indebida" y, en todo caso, en un plazo de 72 horas, salvo que el responsable considere que es improbable que dicha violación de la seguridad constituya un riesgo. En este caso, y en lo que concierne estrictamente al ámbito de la notificación, la obligación del proveedor de servicios en nube se limita únicamente a comunicar cualquier violación de la seguridad a su cliente en cuanto que responsable (art. 33.2 RGPD). En el caso de que el riesgo se considere alto, entonces el responsable deberá notificarlo, ex. art. 34, al interesado sin dilación indebida; salvo que las medidas de protección técnicas y organizativas hayan sido apropiadas y en particular aquellas que hagan ininteligibles los datos; salvo que haya tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concrete el alto riesgo; o salvo que suponga un esfuerzo desproporcionado, en cuyo caso se optará por una comunicación pública o una medida semejante.

Podemos observar por tanto que, sin perjuicio de esa obligación de comunicación al responsable/cliente, lo concerniente a las notificaciones está claramente focalizado en el cliente. En todo caso, al igual que en muchos otros ámbitos que hemos ido viendo, y fundamentalmente como consecuencia de la potencial desigualdad entre las partes, será necesaria e inevitable la colaboración por parte del proveedor, máxime si como hemos apuntado al principio de este apartado, la seguridad constituye el pilar de su negocio.

Particular relevancia puede tener el supuesto de excepción a la comunicación al interesado y más concretamente el referido a la adopción de las medidas técnicas y organizativas que hayan minimizado el riesgo. En muchas ocasiones estas vendrán dadas y aportadas por el proveedor cloud y no tanto por el cliente propiamente dicho. Cabe subrayar que, como todo instrumento jurídico, el uso de conceptos abiertos impide en muchas ocasiones saber con certeza cuándo se tiene que dar la notificación. Resulta a este respecto sumamente práctico el Dictamen 08/2014 del Grupo de trabajo del artículo 29 sobre notificaciones de violaciones de datos personales donde al hilo de la referida Directiva 2002/58, y tras recordar que la razón de ser de la exención de notificación a los interesados es que medidas adecuadas pueden reducir los riesgos de privacidad residuales a un nivel insignificante, señalaba supuestos que exigían de notificación bajo el amparo general de la normativa de protección de datos[803]. En todo caso, sería muy conveniente que se articulasen desde las autoridades de protección de datos guías de protocolización de los incidentes de seguridad que vayan más allá de la mera norma, que desciendan a aspectos prácticos, que aporten en definitiva seguridad jurídica al cliente de que está actuando correctamente. La guía de "Cómo gestionar una fuga de información en un despacho de abogados"[804], referida al ámbito de la abogacía en concreto es un exponente de aquello a lo que nos estamos refiriendo.

2.3.3 La tranquilidad del cliente de la nube: certificaciones y auditorías

Sin embargo, con base en el esquema de responsabilidad que normativamente está establecido, no basta con que el proveedor facilite las medidas de seguridad necesarias, sino que además es necesario e importante que el cliente tenga la posibilidad de verificar que las mismas se cumplen. Al respecto existen diversos mecanismos que la AEPD ha recogido en su Guía de Seguridad antes citada y que son lógica proyección de lo previsto en las normas. Así, siguiendo a la Agencia, se recuerda que el cliente debe tener la opción de comprobar las medidas de seguridad, incluidos los registros que permiten conocer quién ha accedido a los datos de los que es responsable; o bien el proveedor de cloud computing le acredita que dispone de una certificación de seguridad adecuada; o puede acordarse que un tercero

[803] ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 08/2014 on Personal Data Breach Notification. 25 de marzo de 2014. Disponible en web: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[804] Esta guía, impulsada por la Agencia, el Instituto de Ciberseguridad y el Consejo General de la Abogacía Española, ha sido publicada en octubre de 2016. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, INCIBE, CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA. Cómo gestionar una fuga de información en un despacho de abogados. Octubre 2016. Disponible en web: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/INCIBE_AEPD_Gestionar_fuga_de_informacion.pdf

independiente audite la seguridad, en cuyo caso debe conocerse la entidad auditora y los estándares reconocidos que aplicará; El cliente debe ser informado diligentemente por el proveedor de cloud sobre las incidencias de seguridad que afecten a los datos de los que el propio cliente es responsable, así como de las medidas adoptadas para resolverlas o de las medidas que el cliente ha de tomar para evitar los daños que puedan producirse (p. ej. informar a sus propios clientes sobre cómo proteger su información personal); y a ello añade que el cifrado de los datos personales es una medida que debe valorarse positivamente.

Tal y como ya hemos visto, muchas de las medidas que se señalan aquí como recomendadas por la Agencia han sido contempladas expresamente incluso de manera más exigente por el RGPD, como por ejemplo el régimen de notificaciones, por lo que en todo caso será necesario adaptase a las previsiones de este. En realidad, cabe reflejar que la Agencia las ha contemplado porque muchas de ellas se derivan de las previsiones ya vigentes en el actual ROPD.

En esta línea y desde el punto de vista doctrinal, Montero afirma que, desde el punto de vista de la LOPD y su Reglamento, el cliente deberá tener la opción de comprobar las medidas de seguridad, o bien el proveedor de cloud computing debe acreditarle que dispone de una certificación de seguridad adecuada, o incluso puede acordarse que un tercero independiente audite la seguridad[805].

En la misma línea, el Grupo de Trabajo del artículo 29, en su tantas veces citado Dictamen 05/2012, ha señalado en sus recomendaciones y conclusiones, por un lado que la verificación independiente o la certificación por terceros que gocen de reconocido prestigio puede ser un medio creíble para que los proveedores demuestren el cumplimiento de sus obligaciones; y por otro, ha afirmado que la realización de auditorías individuales de datos alojados en un medio de servidores virtualizados con múltiples operadores puede ser poco práctica desde el punto de vista técnico y puede en algunos casos aumentar los riesgos para los controles físicos y lógicos de seguridad de las redes; añadiendo que en dichos casos podrá considerarse que la auditoría por un tercero de reconocido prestigio elegido por el

[805] MONTERO, S. Cumplimiento, seguridad y control en la nube ¿Es posible? *Blog KPMG Ciberseguridad*. 6 de junio de 2015. Disponible en web: http://www.kpmgciberseguridad.es/cumplimiento-seguridad-y-control-en-la-nube-es-posible/

responsable del tratamiento puede sustituir al derecho de un responsable del tratamiento de realizar una auditoría[806].

A mayor abundamiento, el referido Dictamen 05/2012 ha señalado que la adopción de normas y certificaciones específicas sobre protección de la intimidad es esencial para establecer una relación de confianza entre los proveedores, los clientes y los interesados, y que dichas normas y certificaciones deben cubrir las medidas técnicas (como la localización de los datos o la codificación), así como los procesos seguidos por los proveedores de servicios de computación en nube para garantizar la protección de los datos (tales como políticas de control del acceso, controles de acceso o copias de seguridad)[807]. En el plano nacional, la autoridad irlandesa por ejemplo señala que la certificación puede ser un medio útil para demostrar el cumplimiento con los requerimientos de la normativa de protección de datos, en la que se señala que la certificación indica que los controles de seguridad de los datos han sido sometidos a una auditoría o revisión por un tercero con base en un estándar reconocido. Y añade que, en el contexto de la computación en nube, los clientes deberían observar si el proveedor les puede facilitar una copia de la certificación o de la auditoría[808].

De hecho, se puede decir que los sistemas de certificación son un esquema práctico y más razonable teniendo en cuenta la creciente asimetría entre proveedor y cliente, y más si cabe cuando exista una natural tendencia del proveedor a salvaguardar la discreción tecnológica y física de sus sistemas de seguridad. Como señala Cotino Hueso, "la mejor práctica es que contractualmente se acepten certificaciones y auditorías de terceros con plena transparencia"[809]. En definitiva, la certificación y la auditoría, íntimamente conectadas por cuanto la primera exige de la segunda, sea propia o elaborada por terceros, es un sistema razonable a aplicar en los entornos *cloud* salvando las barreras de asimetría antes mencionadas. Así parece corroborarlo el Grupo de Trabajo del artículo 29 que, en su Dictamen 05/2012, afirma que "la certificación por terceros que gocen de reconocido prestigio puede ser un medio creíble para que los proveedores demuestren el cumplimiento de sus obligaciones…Dicha certificación indicaría, como mínimo, que los controles de protección de datos han sido objeto de una auditoría o revisión con respecto a una norma reconocida que cumple los requisitos expuestos en el presente dictamen, por una organización tercera que

[806] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 05/2012, sobre computación en nube. Ob. Cit. p. 25.
[807] *Idem.* p. 25 y 26.
[808] DATA PROTECTION COMMISSIONER. Data protection Guidance. Ob. cit.
[809] COTINO HUESO, L. Algunas cuestiones clave de protección de datos en la nube: hacia una regulación nebulosa. ob. cit. p. 98.

goce de reconocido prestigio. En el contexto de la computación en nube, los clientes potenciales deben examinar si los proveedores de servicios en la nube pueden presentar una copia de este certificado de auditoría realizado por un tercero o una copia del informe de auditoría que verifique la certificación, incluso con respecto a los requisitos que figuran en el presente dictamen"[810].

En lo que concierne al mecanismo de certificación, se puede definir como una acción llevada a cabo por una entidad independiente de las partes interesadas mediante la que se manifiesta que una organización, producto, proceso o servicio, cumple los requisitos definidos en unas normas o especificaciones técnicas[811].

En el ámbito específico de la "nube", y sin perjuicio de aquellas que genéricamente giran en torno a la seguridad de la información (las normas 27000 ISO/IEC), especial mención hay que hacer a la norma ISO/IEC 27018[812] que constituye el primer estándar internacional sobre privacidad en la nube. Se trata de una norma de particular relevancia a nuestros efectos por dos motivos[813]: se basa, fundamentalmente, en leyes y regulaciones emitidas en la Unión Europea; y está basado en el esquema en el que el cliente del servicio es el responsable del tratamiento, es decir, quien decide sobre el tratamiento de los datos; y el proveedor es el encargado del tratamiento y debe tratar dichos datos siguiendo las instrucciones del cliente. Es decir, se basa en el esquema B2B al que nos hemos venido refiriendo. Sus cuatro objetivos fundamentales son[814]: servir como herramienta para que los proveedores cumplan con las obligaciones de protección de datos aplicables; permitir a dichos proveedores ser más transparentes frente a los clientes; asistir a los proveedores y a los clientes en la negociación de los contratos de servicios cloud; y proveer a los clientes con mecanismos de auditoría. Cabe reseñar al respecto, que el Grupo de Trabajo del artículo 29 ha venido a catalogar esta norma como una buena colección de controles no obligatorios, no exhaustivos y no maximalistas que pueden ser implementados; pero subraya que no ha sido construida para ser utilizada como un documento autónomo para certificación, sino que puede ser

[810] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 05/2012, sobre computación en nube. Ob. Cit. p. 25.
[811] http://www.aenor.es/aenor/certificacion/procesos/proceso_certificacion_aenor.asp#.V_3Bj_CLS00
[812] La denominación oficial completa es Norma ISO/IEC 27018:2014 Tecnología de la información. Técnicas de seguridad. Código de práctica para la protección de información personal identificable (IPI) en nubes públicas que actúan como encargados del tratamiento.
[813] AENOR. Norma ISO/IEC 27018. *Revista AENOR*. 20 de noviembre de 2015. p. 21. Disponible en web: http://www.aenor.es/revista/pdf/nov15/20nov15.pdf
[814] BIRD&BIRD. Cloud computing and privacy series: security requirements and guidance. 1 de diciembre de 2014. Disponible en web: http://www.twobirds.com/en/news/articles/2014/global/cloud-computing-series-security-requirements-and-guidance

utilizado, precisamente, con la referida ISO/IEC 27001[815]. A ellas se podrían añadir otras normas ISO que están ya tramitadas o en proceso de tramitación, caso de la ISO/IEC 27017:2015 Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la información. Directrices sobre controles de seguridad de la información para utilización en servicios de computación en la nube basadas en ISO/IEC 27002; o la ISO/IEC 27036, que es un estándar múltiple para la seguridad de la información en la gestión de las relaciones con proveedores y que cubre los servicios de *outsourcing* y, lógicamente, los de *cloud computing*. En fin también cabría sumar en el plano general la UNE-ISO 19600:2015 Sistemas de gestión de compliance. Directrices, que es una herramienta al servicio de las organizaciones para detectar y gestionar los riesgos a los que se enfrentan por posibles incumplimientos de sus obligaciones.

Igualmente se pueden tener en cuenta otras directrices impulsadas por la Unión Internacional de Telecomunicaciones como la directriz de seguridad para la computación en nube en las áreas de telecomunicaciones (ITU-T X.ccsec), el marco y requerimientos de seguridad del entorno de servicios de telecomunicaciones basados en la nube (ITU-T X.srfctse), requerimiento de gestión de identidad en cloud computing (ITU-T X.idmcc), marco de plataforma de servicio segura para red virtual (ITU-T X.fsspvn), o los requerimientos funcionales de seguridad para entornos de aplicación SaaS (ITU-T X.sfcse)[816]. En Estados Unidos cabe mencionar también la *Statement on Auditing Standards (SAS) No. 70*[817] que sin embargo, como apuntan Beltrán Pardo y Sevillano Jaén[818], se está viendo sustituida. A ellas podemos añadir, siguiendo a Puyol Montero[819], las normas *Systrust* y *Webtrust*, también, al igual que la anterior, del Instituto Americano de Auditores Públicos Certificados (AICPA), o la Certificación según la *Federal Information Security Manager Act* (FISMA): NIST SP 800-37 Guía para la certificación y acreditación de sistemas de información federales[820].

En el ámbito de la industria, cabe mencionar la *CSA STAR Certification* que consiste en una evaluación de seguridad de un proveedor llevada a cabo por un tercero independiente. Se

[815] ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing., 22 de septiembre 2015. Disponible en web: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf
[816] INTERNATIONAL TELECOMMUNICATIONS UNIT. Privacy in Cloud Computing. marzo de 2012. Disponible en web: https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf
[817] Para más información sobre SAS 70, ver http://sas70.com/sas70_overview.html
[818] BELTRÁN PARDO, M. y SEVILLANO JAÉN. F. *Cloud Computing, tecnología y negocio*. Ob. cit. p. 85.
[819] PUYOL MONTERO, J. ob. cit. p. 213.
[820] Acceso al texto completo en el siguiente enlace: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

trata de una certificación tecnológicamente neutral que aprovecha los requisitos de los estándares del sistema de gestión de la ISO/IEC 27001 antes citada, junto con el CSA Cloud Controls Matrix, un conjunto específico de criterios que mide los niveles de capacidad del servicio *cloud*[821]. También dentro del ámbito de la industria, situaríamos la StarAudit de Eurocloud[822].

También las auditorías han jugado tradicionalmente un papel clave en materia de seguridad. Así se puede ver cómo en la normativa española de protección de datos se contempla la auditoría como una de las medidas de seguridad. En concreto el art. 96 ROPD la exige a partir del nivel medio, señalando que deberá darse cada dos años o bien cuando se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas. La auditoría, que puede ser externa o interna, tiene como objetivo dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias, incluyendo igualmente los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas. En el marco del tratamiento de datos por cuenta de terceros mediando transferencias internacionales, también se observa la importancia de este instrumento. Así, la cláusula 5.f) de la Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, 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, contempla la obligación por parte del importador de ofrecer a petición del exportador de datos sus instalaciones de tratamiento de datos para que se lleve a cabo la auditoría de las actividades de tratamiento cubiertas por las cláusulas. Esta será realizada por el exportador de datos o por un organismo de inspección, compuesto por miembros independientes con las cualificaciones profesionales necesarias y sujetos a la confidencialidad, seleccionado por el exportador de datos y, cuando corresponda, de conformidad con la autoridad de control. En fin, similares previsiones se recogen para el subencargado en las cláusulas 5.f) y 8 del Modelo de cláusulas contractuales AEPD para transferencias internacionales de datos entre encargado y subencargado del tratamiento.

[821] Para más información sobre esta certificación, ver https://cloudsecurityalliance.org/star/certification/
[822] Para más información sobre esta certificación, ver https://staraudit.org/home/about.html

En el caso que nos ocupa, la computación en nube, su trascendencia es mayor si cabe. Hay que tener en cuenta, como señala la CSA, que estamos ante un entorno dinámico que evoluciona y cuyas partes deben adaptarse. Por ello recomiendan un monitoreo periódico, un testeo y una evaluación de los servicios de cara a asegurar que la privacidad exigida y las medidas de seguridad son utilizadas, que los procesos y las políticas son seguidas[823]. La AEPD en su Guía lo recuerda igualmente y el INTECO señalaba que, si los prestadores de servicios tradicionales se hallan sujetos a auditorías externas y certificaciones de seguridad, los proveedores de servicios en la nube también deben acogerse a este tipo de prácticas. Añadiendo que si se negasen a este tipo de auditorías no se les debería confiar los datos sensibles de la empresa[824]. En fin, en su Informe sobre Cloud Compliance que elaboró el Capítulo español de la referida CSA, se afirmaba que en los entornos de computación en la nube es importante que cliente y proveedor de los servicios sean conocedores de los niveles de riesgo de ambas partes[825].

El RGPD generaliza este mecanismo de auditoría y no lo vincula a una medida de seguridad en concreto. Así, tal y como ya se ha visto, forma parte del contenido obligatorio del contrato que el encargado pondrá a disposición del responsable toda la información necesaria para la realización de auditorías, incluidas inspecciones, por parte del cliente o de otro auditor autorizado por este (art. 28.3.h)). Por otro lado, el contenido de las BCR incluye auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado (art. 47.2.j))

En cuanto al cómo se realiza la auditoría, con base en la referida Guía de Seguridad, de manera genérica se pueden apuntar cuáles son las comprobaciones a realizar[826]:

[823] CLOUD SECURITY ALLIANCE. Security Guidance for Critical Areas in Cloud Computing. V3.0 2011. página 38. Disponible en web: https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf
[824] INTECO. Riesgos y amenazas en Cloud Computing. ob. cit. p. 16,
[825] CLOUD SECURITY ALLIANCE. SPANISH CHAPTER. Cloud Compliance Report. 1 de mayo de 2011. p. 81. Disponible en web: http://clubgertech.unavarra.es/getfile.php?file=Jornadas/11CloudComputing/des144_Cloud_Compliance_Report_CSA-ES_V.1.0.pdf
[826] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía de Seguridad de Datos. Ob. cit. p. 40 y siguientes.

Alcance
•cuáles son los ficheros con datos de carácter personal objeto de la auditoría, tratamientos sobre los mismos, sistemas de tratamiento, procedimientos
Planificación
•recursos necesarios para llevar a cabo la auditoría, las fuentes de información, la ubicación del fichero o las instalaciones
Recolección de los datos
•Relación de ficheros, estructura y contenido. •Políticas de seguridad y procedimientos (registro de incidencias, copias de respaldo y recuperación, •Identificación y autorización, borrado de soportes, cifrado, etc.). •Documento de Seguridad y auditorías anteriores (si las hubiese). •Diseño físico y lógico de los sistemas de información. •Relación de usuarios, accesos autorizados y sus funciones. •Inventario de soportes y registro de entrada y salida de soportes. •Registros de acceso e informes de revisión de los mismos. •Entrevistas a usuarios, técnicos de sistemas, responsables, etc. •Inspección visual.
Evaluación de las pruebas

Fuente: elaboración propia

Y respecto a quién deba llevar a cabo la Auditoría, en el esquema tradicional se trata de un derecho de que dispone el responsable. Sin embargo, como señalaba el Grupo de Trabajo en su Dictamen sobre computación en nube, la realización de auditorías individuales de datos alojados en un medio de servidores virtualizados con múltiples operadores puede ser poco práctico desde el punto de vista técnico y puede en algunos casos puede aumentar los riesgos para los controles físicos y lógicos de seguridad de las redes. En tales casos, podrá considerarse que la auditoría por un tercero de reconocido prestigio elegido por el responsable del tratamiento puede sustituir al citado derecho de un responsable del tratamiento de realizar una auditoría[827]. A ello cabe añadir dos aspectos relevantes en cuanto al proceso de auditoría y que han sido subrayados por la Agencia Española de Protección de Datos en sendos informes: por un lado que, como ya se ha apuntado y por su lógica conexión, podría suplirse la realización de una auditoría por el responsable por una certificación siempre que ésta cubra tanto las medidas técnicas (tales como la localización de los datos o la codificación) como los procesos seguidos por los proveedores de servicios

[827] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 05/2012, sobre computación en nube. ob. cit. p. 25.

de computación en nube para garantizar la protección de los datos[828]; y por otro, que la entidad auditora puede ser contratada por el proveedor, siempre y cuando sea una entidad enteramente independiente del aquél y se encuentre debidamente certificada o acreditada, tanto en lo que se refiere a su independencia como en lo que atañe a sus procedimientos de actuación, y se permita, en todo caso, al cliente manifestar su opinión y cómo acceder a los resultados del informe de auditoría[829].

Desde el punto de vista formal, y como ya se ha señalado más arriba y también en otros apartados de este capítulo, las medidas de seguridad constituyen uno de los elementos a incluir en el contrato. Resulta lógico que, si venimos subrayando en este apartado la importancia de las medidas de seguridad como elemento fundamental de las relaciones entre las dos partes, se incluya su contenido. Así lo establece el segundo párrafo del artículo 12.2 LOPD cuando señala expresamente que "En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar". En la misma línea, el RGPD, en su art. 28.3.c) dice que en el contrato se recogerá que el encargado (en nuestro caso el proveedor) tomará todas las medidas necesarias de conformidad con el artículo 32. Del mismo modo, las cláusulas contractuales tipo lo han recogido en su contenido. De este modo el apartado c) de la cláusula 4.3 recogida en la Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, 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 dice "El exportador de datos acuerda y garantiza lo siguiente: "el importador de datos ofrecerá garantías suficientes en lo que respecta a las medidas de seguridad técnicas y organizativas especificadas en el apéndice 2 del presente contrato". En la vertiente del importador, en nuestro caso el proveedor de servicios cloud, "…acuerda y garantiza lo siguiente: c) ha puesto en práctica las medidas de seguridad técnicas y organizativas que se indican en el apéndice 2 antes de efectuar el tratamiento de los datos personales transferidos". También en el marco de las BCR se hace

[828] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Informe 0464/2012. Disponible en web: https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2012-0464_Contrataci-oo-n-de-servicio-de-cloud-computing-por-cl-ii-nica-m-ee-dica.pdf

[829] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Informe 0157/2012. Disponible en web: https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2012-0157_Especialistas-cl-aa-usulas-contractuales-en-cloud-computing..pdf
Recordemos que este último informe, como se ha visto ya en este capítulo, fue uno de los determinantes a la hora de dar lugar a la construcción de unas cláusulas específicas para las transferencias internacionales entre encargado y subencargado.

una mención expresa a la inclusión de las medidas de seguridad por parte de los miembros del grupo o corporación. Así, el Grupo de Trabajo del art. 29, en su Documento 02/2012, establece un listado con elementos y principios que deberán contemplar las BCR y recoge referencias a las seguridad en diferentes momentos: en concreto, en la vinculatoriedad a todos los miembros del grupo señala que "Las BCR deberán recoger expresamente que todos los miembros del Grupo y los empleados deberán respetar las instrucciones concernientes al tratamiento de los datos y las medidas de seguridad y confidencialidad tal y como se establezcan en el Acuerdo de Servicio (artículo 17); mientras que en los principios de las BCR se recoge el de seguridad: encargados y subencargados deben cumplir con las medidas organizativas y de seguridad que, al menos, cumplan con los requisitos que exija la ley aplicable al responsable y cualquier medida particular existente especificada en el Acuerdo de Servicio. Encargados y subencargados deben informar inmediatamente de cualquier quiebra de seguridad al responsable. Y, por último, dentro de estas mismas BCR se señala que para las BCR para encargados deben indubitadamente estar ligadas al Acuerdo de Nivel de Servicio firmado con cada cliente[830].

Como se puede deducir de la transcripción, otra de las vertientes que hemos tratado y que sin duda tiene su particular incidencia en el ámbito de las medidas de seguridad es la referida a la subcontratación, es decir, a los casos en los que el proveedor recurre a proveedor, es decir, a la subcontratación. El elemento dinámico que conlleva la computación donde como ya se ha estudiado existe una fuerte presencia de subencargados del tratamiento, conlleva que la salvaguarda de la seguridad informe la totalidad de la cadena del tratamiento. Como recordaba el INTECO para la creación de un servicio *cloud* interviene multitud de software de distintos proveedores, es decir, son entornos complejos por lo que se ha de poner especial atención a las posibles vulnerabilidades del mismo e implantar procedimientos de parcheado[831]. En sus guías, la Agencia Española de Protección de Datos hace hincapié en esta vertiente, recordando que el proveedor debe asumir en el contrato que los subcontratistas le ofrecen garantías jurídicas para el tratamiento de los datos equivalentes a los que él mismo asume[832]. Y añade al respecto que será necesaria la celebración de un contrato entre el prestador de servicios de cloud computing y los subcontratistas con

[830] ARTICLE 29 DATA PROTECTION WORKING PARTY. Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules. 6 de junio de 2012. Disponible en web: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf
[831] INTECO. Riesgos y amenazas en *Cloud Computing.* ob. cit. p. 30.
[832] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía para clientes que contraten servicios de Computing. ob cit. p. 14.

garantías equivalentes a las incluidas en el contrato con el cliente[833]. En fin, estas lógicas cautelas se contemplan también en los clausulados tipo, y así, en el Modelo de cláusulas contractuales AEPD para transferencias internacionales de datos entre encargado y subencargado del tratamiento[834] se recoge que el subencargado ofrece garantías suficientes en lo que respecta a las medidas de seguridad técnicas y organizativas, que se ha verificado que dichas medidas resultan apropiadas para proteger los datos, que dichas medidas garantizan un nivel de seguridad apropiado a los riesgos que entraña el tratamiento y la naturaleza de los datos que han de protegerse, habida cuenta del estado de la técnica y del coste de su aplicación; y que se asegura de que dichas medidas se llevan a la práctica.

De lo visto a lo largo del presente apartado podemos concluir que las afirmaciones que se han llevado a cabo al principio son correctas. La seguridad constituye, hoy día más si cabe, uno de los elementos fundamentales que informan la normativa de protección de datos. Está en las máximas prioridades de las autoridades oficiales y de la propia industria. Existen normas o al menos principios que son perfectamente trasladables, a través de los lógicos ajustes, al esquema de la computación en nube. Bien es cierto que se ha perdido una oportunidad para introducir en el RGPD disposiciones específicas referidas a la computación en nube, aunque el propio desarrollo tecnológico y la diferente velocidad con respecto a la normativa hacen que ajustes normativos demasiado detallados estén condenados a la caducidad en sí misma. A día de hoy, y con base en la tendencial asimetría que existe entre las partes, parece conveniente que los mecanismos de auditoría y certificación sean los más adecuados, siempre que estos se ajusten a los esquemas normativos fijados y con un cierto grado de supervisión por parte de las autoridades de protección de datos, con las finalidades instrumentales de salvaguardar el negocio del proveedor y dotar de una cierta seguridad jurídica al cliente en cuanto que responsable; así como una finalidad última de proteger el derecho fundamental de los interesados. En todo caso, cualquier sistema que se implante tiene que ir acompañado en la nube por un cierto grado de dinamismo y flexibilidad, o de escalabilidad en la seguridad si se prefiere. Se trata en definitiva de garantizar los equilibrios entre el nivel de riesgo y el nivel de seguridad, y entre este y el estado de la técnica y los costes del sistema. La seguridad absoluta no existe y no se le puede pedir a ningún

[833] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Orientaciones para prestadores de Servicios de Cloud Computing. ob. cit. p. 7.

[834] Acceso al texto del clausulado tipo en el siguiente enlace: https://www.agpd.es/portalwebAGPD/resoluciones/autorizacion_transf/common/pdfs/MODELO-DEFINITIVO-AEPD_Contrato-encargado-subencargado-21-03-2012.pdf

proveedor, pero la articulación de sistemas que minimicen los riesgos con base en el estado de la técnica, de protocolos de actuación ante posibles vulnerabilidades, de una asunción de responsabilidad en la cadena de subcontrataciones y de una implicación de todos los actores, contribuirá a hacer de la computación en nube una tecnología de éxito.

3 El acceso por las autoridades públicas a los datos en la nube

3.1 Encuadramiento constitucional

Cualquier referencia a que una autoridad pública acceda a la información personal exige inevitablemente, un encuadramiento constitucional, por cuanto el contenido de los derechos fundamentales se ve tensado cuando de la potencial legitimidad de la actuación de los poderes públicos se trata.

En este punto, y sin perjuicio de todo lo que ya se ha mencionado al respecto en el primero de los capítulos de este trabajo, no se puede obviar que el acceso a la información en dispositivos electrónicos, sean o no accesos remotos, se trate o no de la nube, siempre ha de realizarse con pleno sometimiento a los criterios que la jurisprudencia ha construido desarrollando los derechos fundamentales recogidos en la Constitución en relación con otras injerencias, también en el ámbito de los sistemas de información y de las telecomunicaciones [835] . En palabras de Velasco Nuñez, "Nos encontramos [en la investigación de los delitos informáticos], como en pocos otros supuestos, ante el área de protección constitucional más sensible de los derechos fundamentales de la persona del investigado y por ello, dentro de la esfera de defensa más garantista posible , donde debe el Juez , como en ningún otro campo, preservar su imparcialidad y sólo permitir el avance de medidas tan intrusivas de la privacidad en la investigación, cuando la pulsión entre los intereses sociales y los individuales se decanten especialmente por los primeros"[836].

Efectivamente esta cuestión ha suscitado lógicamente el pronunciamiento de los tribunales y la jurisprudencia ha ido marcando en qué medida se puede acceder al contenido alojado en un dispositivo de dicha naturaleza. Por razones prácticas, volvamos a traer aquí las

[835] DELGADO MARTÍN, J. La prueba electrónica en el proceso penal. *Diario La Ley.* Nº 8167. Sección Doctrina, Año XXXIV. 10 Oct. 2013. Disponible en web: https://peritoit.files.wordpress.com/2013/10/la-prueba-eletronica-en-el-proceso-penal.pdf

[836] VELASCO NUÑEZ, E. Aspectos procesales de la investigación y de la defensa en los delitos informáticos. *Ilustre Colegio de Abogados de Madrid.* Disponible en web: http://web.icam.es/bucket/Aspectos%20Procesales%20de%20la%20Investigacion%20y%20Defensa%20Delitos%20Informaticos.pdf

principales ideas. En el plano europeo, se parte del artículo 8 CEDH, en cuyo párrafo segundo se recuerda que "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 de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás". Con base en ello, el TEDH, así en Sentencia *Iliya Stefanov vs. Bulgaria*[837] recordaba, precisamente en un caso en el que se consideró vulnerado el derecho a la intimidad y en el que se había accedido a datos de ordenadores, la necesidad de que concurrieran los referidos requisitos, siendo de necesaria clarificación el concerniente a "una medida que, en una sociedad democrática". Al respecto el Tribunal recuerda que se debe examinar la concurrencia de salvaguardas efectivas contra el abuso o la arbitrariedad bajo el Derecho nacional y comprobar cómo dichas salvaguardas operan en cada caso específico: la gravedad de la conducta en conexión con el registro y búsqueda efectuados, si se han llevado a cabo bajo una autorización judicial, si esta estaba fundada en una sospecha razonable y si su ámbito de actuación estaba razonablemente limitado. Mismo examen llevó a cabo por ejemplo en la STEDH de 3 de diciembre de 2015 en el caso *Sérvulo & Associados - Sociedade de Advogados, Rl vs. Portugal*[838] donde sin embargo llegó a la conclusión contraria precisamente porque el juez portugués, tras haber visualizado los archivos y los correos electrónicos registrados, ordenó el borrado de 850 por considerarlos privados, cubiertos por el secreto profesional o que no tenían relación directa con el caso.

En definitiva y como conclusión, como resume De la Rosa Cortina, "La jurisprudencia del TEDH exige para justificar injerencias del Estado en la vida privada tres requisitos: 1) legalidad, que la injerencia esté prevista por la ley 2) fin legítimo y 3) necesidad, que la medida sea necesaria en una sociedad democrática para la consecución del fin perseguido". Los derechos fundamentales están presentes en los dispositivos electrónicos y consiguientemente el sacrificio de su contenido para acceder a los datos en ellos contenidos exige, una vez más, de un adecuado criterio de ponderación. A ello se añade, como ha quedado demostrado, que resultan válida la filosofía subyacente a cualquier otro registro, sin

[837] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Sección Quinta). Caso *Iliya Stefanov vs. Bulgaria* Sentencia de 22 de mayo de 2008. Acceso al texto de la Sentencia en el siguiente enlace: http://hrlibrary.umn.edu/research/bulgaria/IStefanov_en.pdf

[838] Consejo de Europa. Tribunal Europeo de Derechos Humanos (Sección Primera). Caso *Sérvulo & Associados - Sociedade de Advogados, Rl vs. Portugal.* Sentencia de 3 de diciembre de 2015. Acceso al texto de la Sentencia en el siguiente enlace: http://hudoc.echr.coe.int/eng#{"itemid":["001-156519"]}

perjuicio de la necesaria adaptabilidad al entorno tecnológico en virtud de lo que, como inmediatamente veremos, nuestro Tribunal Supremo denomina el derecho al propio entorno virtual.

En España, al margen de la última reforma operada en la Ley de Enjuiciamiento Criminal que se analizará, la jurisprudencia lógicamente ha tratado también esta cuestión. A título de ejemplo, y mereciendo la extensión que se recoge, la STS de 17 de abril de 2013[839] recordaba que "La ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de *nomen iuris* propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital".

En el ámbito del Tribunal Constitucional español, la Sentencia quizá más relevante en este punto fue la STC 173/2011 ya mencionada en el primer capítulo, y en la que se recordaba que "Si no hay duda de que los datos personales relativos a una persona individualmente considerados…están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) —por lo que sus funciones podrían equipararse a los de una agenda electrónica—, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de

[839] España. Tribunal Supremo (Sala Segunda de lo Penal). Sentencia 342/2013, de 17 de abril. Disponible en web: http://supremo.vlex.es/vid/438315958

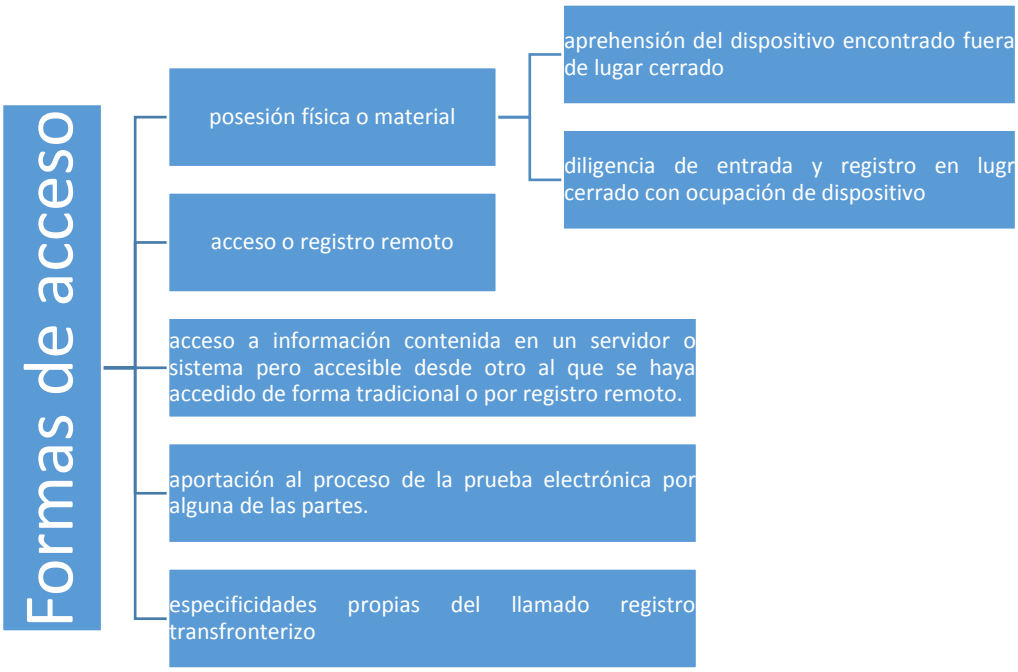
la esfera más íntima del ser humano". Y donde se subrayaba que "cualquier injerencia en el contenido de un ordenador personal —ya sea por vía de acceso remoto a través de medios técnicos, ya, como en el presente caso, por vía manual— deberá venir legitimada en principio por el consentimiento de su titular, o bien por la concurrencia de los presupuestos habilitantes antes citados". Estos presupuestos habilitantes son, como nos recuerda la STC 115/2013, de 9 de mayo, la autorización judicial o bien que "existan razones de necesidad de intervención policial inmediata para la averiguación del delito, el descubrimiento de los delincuentes o la obtención de pruebas incriminatorias, siempre que se respete el principio de proporcionalidad".

Si se observa la doctrina que el Tribunal Constitucional ha ido fijando respecto del acceso al domicilio, se puede llegar a la misma conclusión que apuntábamos más arriba en el plano europeo, y es que a pesar de todas las particularidades y acomodaciones que exige el componente tecnológico, los fundamentos últimos que habilitan la entrada en el domicilio son los mismos que los del acceso a la información en dispositivos: el consentimiento del titular, una resolución judicial motivada y respetuosa con el principio de proporcionalidad o bien los supuestos de flagrante delito (por todas, STC 160/1991, de 18 de julio)[840].

3.2 El acceso remoto a la información: privacidad vs. seguridad

Esta última referencia nos marca las pautas que permiten la posibilidad del acceso al contenido tecnológico, que a su vez puede tener lugar, como se refleja en el siguiente diagrama, de muy diferentes formas:

[840] España. Tribunal Constitucional. Pleno. Sentencia 160/1991 de 18 de julio de 1991. Disponible en web: http://hj.tribunalconstitucional.es/en/Resolucion/Show/1799



Fuente: elaboración propia con base en descripción de Delgado Martín[841]

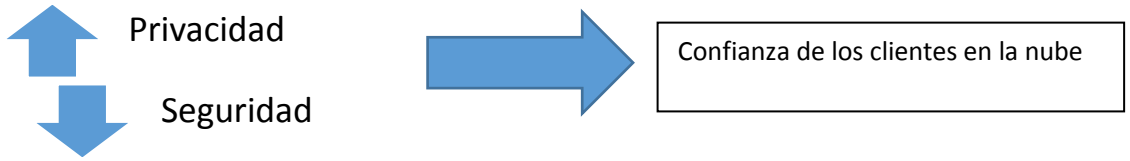
Son precisamente las modalidades de acceso remoto en sentido amplio las que nos ocupan por su potencial vinculación con la nube. Decimos que potencial porque el acceso remoto se puede dar con respecto a dispositivos electrónicos que no almacenen en la nube como un Smartphone, una tableta o un ordenador portátil que simplemente se encuentre en movimiento. Ciertamente es muy frecuente que a su vez este tipo de dispositivos tengan contenido almacenado en la propia nube, algo que ocurre sin duda con respecto del supuesto de acceso a la información contenida en un servidor a través de un dispositivo conectado a la Red, y que alcanza su dimensión más compleja cuando además, el referido servidor se encuentra ubicado más allá de nuestras fronteras. Y es que es aquí donde la polémica y la controversia, así como los problemas jurídicos y la preocupación del cliente, merecen nuestra particular atención.

No es infrecuente, tal y como hemos venido reiterando, que en el marco de la prestación de servicios en nube se produzcan transferencias internacionales de datos, sea en sentido material, esto es incluyendo países de la UE o que tienen el amparo de decisiones de la Comisión Europea, o sea en sentido jurídico. Ello ha provocado que una de las cuestiones

[841] DELGADO MARTÍN, J. La prueba electrónica en el proceso penal. *Diario La Ley.* Nº 8167. Sección Doctrina, Año XXXIV. 10 Oct. 2013. Disponible en web: https://peritoit.files.wordpress.com/2013/10/la-prueba-eletronica-en-el-proceso-penal.pdf

de preocupación sea la posibilidad del acceso por parte de las autoridades de ese tercer país a los datos alojados o tratados en el mismo, y que se puede resumir siguiendo al profesor Walden básicamente en los siguientes interrogantes: a) La norma que da amparo a la actuación por parte de las agencias de investigación y b) el ámbito territorial de actuación y los posibles efectos extraterritoriales[842]. Se trata de una cuestión de honda preocupación tal y como ha puesto de manifiesto en diferentes ocasiones la propia Unión Europea, que ha subrayado que la cuestión de la privacidad y de la protección de datos está cuestionada por medidas excepcionales adoptadas en nombre de la seguridad y de la lucha contra el terrorismo[843].

A la clásica dicotomía entre libertad y seguridad, se une en este caso una dicotomía entre privacidad y seguridad, que tiene como efecto directo la confianza de los clientes en la nube.



Fuente: elaboración propia

Las autoridades de protección de datos, en sus documentos de estudio y análisis de la computación en nube, han puesto de manifiesto, como factor de riesgo para la privacidad, la existencia de este tipo de potestades por parte de las autoridades de terceros países. A título de ejemplo, la Agencia Española de Protección de Datos ha recordado que cuando los datos están localizados en terceros países podría suceder que una Autoridad competente pueda solicitar y obtener información sobre los datos personales de los que el cliente es responsable. En este caso el cliente debería ser informado por el proveedor de esta circunstancia (salvo que lo prohíba la ley del país tercero)[844]. En Francia, la CNIL señalaba

[842] WALDEN, I. Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent. *Queen Mary, University of London Cloud legal Project*. 14 de noviembre de 2011. Disponible en web: http://www.lake-project.net/download/Uk/Data%20Protection%20_%20Right%20to%20be%20Forgotten/Accessing%20Data%20in%20the%20Cloud.%20The%20Long%20Arm%20of%20the%20Law%20Enforcement%20Agent.pdf

[843] EUROPEAN COMMISSION. Directorate-General for Internal Policies. Fighting cyber crime and protecting privacy in the cloud. 2012. Disponible en web: http://www.ptools.com/Blog/Fighting-Cyber-Crime-and-Protecting-Privacy-in-the-Cloud.pdf

[844] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía para clientes que contraten servicios de Cloud Computing. ob. cit. p. 15.

como uno de los principales riesgos de la nube los requerimientos judiciales, particularmente por autoridades extranjeras[845]. También la autoridad suiza recoge como uno de los principales riesgos de la computación en nube que en determinadas circunstancias el proveedor puede ser requerido para permitir a las autoridades y tribunales el acceso a los datos, incluso si los datos no son tratados o almacenados en ese particular país[846]. De igual modo, el Grupo de Trabajo del artículo 29 destaca como uno de los principales riesgos la falta de confidencialidad por lo que respecta a las solicitudes de intervención legal realizadas directamente a un proveedor, y añadía que existe el riesgo de revelación de datos personales a servicios incluso extranjeros sin una base jurídica de la UE válida y, por tanto, dándose una violación de la legislación de la UE sobre protección de datos[847].

En el plano normativo las referencias a las investigaciones policiales, penales y a cuestiones de interés público, defensa nacional, seguridad nacional, etc., también han estado presentes en más de una ocasión. Así, la Directiva 95/46 señalaba claramente en su Considerando 13 que las actividades a que se refieren los títulos V y VI del Tratado de la Unión Europea relativos a la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en el ámbito penal no están comprendidas en el ámbito de aplicación del Derecho comunitario. De similar modo, el Considerando 19 del RGPD dice que la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal por parte de las autoridades competentes a efectos de la prevención, investigación, detección o enjuiciamiento de infracciones penales o de la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública y la libre circulación de estos datos y su prevención, es objeto de un acto jurídico específico a nivel de la Unión. En el primero de los casos, la excepción viene regulada por 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, regula la protección de datos con arreglo al antiguo tercer pilar[848]; que se verá sustituida en mayo de 2018 por la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos

[845] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. Recommendations for companies planning to use Cloud computing services. Ob cit. p. 4.
[846] FEDERAL DATA PROTECTION AND INFORMATION COMMISSIONER (FDPIC). Guide to cloud computing. ob. Cit.
[847] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 05/2012 sobre la computación en nube. ob. cit. p. 7.
[848] Acceso al texto de la Decisión en el siguiente enlace: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:es:PDF

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, y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo[849].

También el RGPD recoge igualmente que por ejemplo a la hora de evaluar el nivel de adecuación de un tercer país, la Comisión debe tener en cuenta su Derecho general y sectorial, incluida la legislación relativa a la seguridad pública, la defensa y la seguridad nacional, así como el orden público y el Derecho penal, tal y como desarrolla su artículo 45.2.a).

La industria está directamente afectada, por cuanto a ella van dirigidos los requerimientos. Es por ello que se ha venido pronunciando respecto a los principios que deben inspirar el acceso a los datos personales por parte de las autoridades públicas[850]: permitir el acceso a la información digital solo en virtud de procesos legales, el derecho de los proveedores tecnológicos a impugnar, exigir rigor de las formas de los procesos legales de obtención de información más sensible, autorizar la divulgación en situaciones de emergencia, apoyar la transparencia, la notificación al usuario, modernizar las leyes que rigen los objetivos adecuados de las solicitudes de datos en la nube, respetar las fronteras internacionales y la soberanía y promover la confianza a través de la seguridad.

En el ya citado en diversas ocasiones, borrador de Código de Conducta elaborado por la industria bajo el paraguas de la Comisión Europea, se contemplan dos tipos de acceso: por un lado, los requerimientos por parte de las autoridades de protección de datos, donde se dice que el proveedor debe cooperar de buena fe con el cliente y asistir al usuario para gestionar cualquier requerimiento por parte de una autoridad de protección de datos competente. Igualmente se dice que debe cooperar de buena fe cuando el requerimiento sea directo por parte de la autoridad de protección de datos, y se recoge la obligación de notificarlo al cliente de la manera más expeditiva posible, salvo que dichas notificaciones estén prohibidas por ley. En segundo lugar, y en el campo que nos ocupa, se contemplan los requerimientos gubernamentales o de agentes de la autoridad y se señala igualmente que el proveedor informará al cliente de la manera más expeditiva posible de cualquier

[849] Acceso al texto de la Directiva en el siguiente enlace: https://www.boe.es/doue/2016/119/L00089-00131.pdf

[850] MICROSOFT. Recomendaciones sobre la política El acceso gubernamental a los datos. Disponible en web: https://news.microsoft.com/cloudforgood/_media/downloads/es/government-access-to-data-es.pdf

requerimiento jurídicamente obligatorio que reciba para revelar datos, salvo que esté prohibido, como por ejemplo por la normativa penal, de cara a preservar la confidencialidad de la investigación. A mayor abundamiento, se subraya que, antes de responder a cualquier requerimiento por parte de un tribunal o de una autoridad administrativa de un tercer país para transferir o revelar datos, el proveedor debe verificar si el requerimiento está basado en un acuerdo internacional en vigor entre el país requirente y la UE o un Estado miembro, sin perjuicio de otros fundamentos para transferir fijados por la normativa de protección de datos.

Precisamente en el seno de la industria, cabe afirmar que la posibilidad de acceso por parte de las autoridades públicas es una cláusula frecuente en los términos y condiciones de uso de los servicios en nube. Además suele seguir el criterio fijado por el Grupo de Trabajo del artículo 29, que en su dictamen sobre computación en nube recordaba la obligación de notificar al cliente toda solicitud jurídicamente vinculante de divulgar datos personales presentada por las autoridades policiales o judiciales a menos que esté prohibido; por ejemplo en virtud del Derecho penal para mantener la confidencialidad de una investigación policial[851]. Veamos algunos casos concretos. Cuando en junio de 2011 se produjo el lanzamiento de Microsoft Office 365, fue acompañado de expresiones preocupantes de que Microsoft no garantizaba que los datos de los consumidores europeos no pudieran ser objeto de acceso por parte de las autoridades norteamericanas[852]; en sus términos y condiciones de servicio de ICloud Apple (versión 1 de agosto de 2013) señalaba "Usted reconoce y acepta que Apple, sin responsabilidad para usted, puede acceder, usar, conservar y/o revelar la información y el Contenido de su Cuenta a las autoridades policiales, funcionarios de gobierno, y/o terceros, en la medida que Apple determine necesaria o conveniente, si así se le solicita legalmente o en la creencia de buena fe de que dicho acceso, uso, revelación o conservación es razonablemente necesario para: (a) cumplir procesos o solicitudes legales; (b) hacer cumplir este Contrato, incluyendo la investigación de cualquier posible infracción relacionada con las mismas; (c) detectar, impedir o de otro modo solucionar problemas de seguridad, fraudes o problemas técnicos; o (d) proteger los derechos, la propiedad o la seguridad de Apple, sus usuarios, un tercero o el público conforme a lo que exija o permita la legislación; Dropbox (versión de 12 de febrero de 2016) señala igualmente que "Podríamos compartir información tal y como se describe en las siguientes secciones, pero no la venderemos a terceros con fines publicitarios ni de ningún otro tipo. *Fuerzas del orden*.

[851] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 05/2012 sobre la computación en nube. 1 de julio de 2012. Ob. cit. p.16.
[852] Tomado de WALDEN, I. ob. Cit.

Podríamos revelar tu información a terceros si determinamos que dicha revelación es razonablemente necesaria para (a) cumplir obligaciones legales; (b) proteger a cualquier persona en riesgo de muerte o lesiones graves; (c) impedir fraudes o usos indebidos de Dropbox o que afecten a nuestros usuarios; o (d) proteger los derechos de propiedad de Dropbox".

3.3 Los proveedores americanos, *Privacy Shield* y la realidad en Europa

Es precisamente la preponderancia de la nacionalidad norteamericana de los grandes proveedores de este tipo de servicios[853], lo que ha provocado que el principal foco de conflicto para el gran público se haya situado en Estados Unidos. A ello se añade un segundo argumento y es que como se ha subrayado desde instituciones como el Consejo de Europa, en el caso de Estados Unidos, no estamos hablando del acceso a los datos como consecuencia de investigaciones criminales o de seguridad nacional, sino que se han dado escándalos que, bajo el paraguas precisamente de la seguridad nacional, han dado lugar a vigilancias masivas[854].

Es cierto que en Estados Unidos existen normas que dan una gran accesibilidad a los datos por parte de sus autoridades. No obstante, es de justicia subrayar que en realidad esta

[853] Por ejemplo, el número combinado de visitantes únicos a *Microsoft Hotmail, Google Gmail and Yahoo! Mail* desde países europeos en junio de 2012 era superior a los 227 millones, eclipsando los números del resto de proveedores. El número combinado de usuarios europeos únicos que accedieron a Facebook y a Facebook Mobile en marzo de 2012 fue de 196,5 millones, haciendo de Facebook la red social más grande en Europa. Google es el motor de búsqueda líder con 90,2% de los usuarios de internet a nivel mundial. El servicio de mensajería móvil americano What's App fue utilizado por el 91% de los usuarios de IPhone en Alemania en junio de 2013. Tomado de EUROPEAN COMMISSION. Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EUU.S. Data Flows, COM (2013) 846 final, 27 de noviembre de 2013. Disponible en web: http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf

[854] COUNCIL OF EUROPE. T-CY Cloud Evidence Group. Criminal justice access to data in the cloud: challenges. 26 de mayo de 2015. Disponible en web: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2015/T-CY(2015)10_CEG%20challenges%20rep_sum_v8.pdf

posibilidad existe en muchos países[855], y en algunos con normas muy similares[856]. Buena prueba de lo dicho es que de una manera indirecta el propio Grupo de Trabajo del artículo 29 reconoce esta realidad al recordar que "los datos personales tratados en la nube pueden ser objeto de solicitudes de intervención legal por parte de las autoridades policiales o judiciales de los Estados miembros de la UE y de terceros países"[857] y lo mismo se puede decir del Parlamento Europeo que en 2013 reiteraba su grave preocupación no solo por la revelación de los programas de vigilancia de la Agencia de Seguridad Nacional de los EE. UU., sino también de programas similares utilizados por los servicios de inteligencia de varios Estados miembros[858]. Por su actualidad y por sus previsiones, merece destacarse la Ley de Poderes de Investigación *(Investigatory Powers Act* y conocida también como *Snooper's Charter*) de finales de noviembre de 2016[859] que no solamente actualiza normativa existente, sino que introduce nuevos poderes. En lo que nos ocupa, se recoge por ejemplo la obligación por parte de las compañías telefónicas y de internet para que almacenen los historiales de navegación durante doce meses y le otorgan a la policía, los servicios de seguridad y las agencias oficiales un acceso sin precedentes a los datos. También otorga a los servicios de seguridad y la policía nuevos poderes para piratear ordenadores y teléfonos y obliga a los proveedores a ayudar en dicha tarea. También se contempla la posibilidad de recoger datos de comunicaciones en masa. O por ejemplo la posibilidad de exigir a las compañías que

---

[855] MAXWELL, W. y WOLF, F.CH. A Global Reality: Governmental Access to Data in the Cloud A comparative analysis of ten international jurisdictions. *A Hogan Lovells White Paper.* Disponible en web: http://www-05.ibm.com/ch/services/documents/sce/br-government-access-to-cloud-data.pdf
En este documento se analizan los casos de Australia, Canadá, Dinamarca, Francia, Alemania, Irlanda, Japón, España, Reino Unido y Estados Unidos. Idénticas afirmaciones a las contempladas respecto de estos países se contemplan en el caso de Dinamarca, KROMMAN REUMERT. Government Access to Information in the Cloud. marzo de 2012. Similares afirmaciones se pueden observar en LINKLATERS. Law Enforcement and Cloud Computing. octubre de 2011. Disponible en web: http://www.linklaters.com/Insights/law-enforcement-cloud-computing/Pages/Index.aspx Este documento se centra fundamentalmente en Francia, concretamente en la Ley 2001-1062, de 15 de noviembre de 2001, relativa a la seguridad cotidiana, y en la Ley 2011-267, de 14 de marzo de 2011 relativa a asuntos de seguridad nacional; y en España, y más concretamente en la Ley 12/2003, de 21 de mayo, de bloqueo de la financiación del terrorismo. Por obvias razones, no está contemplada la última reforma de la Ley de Enjuiciamiento Criminal a la que nos referiremos al final de este apartado.

[856] Es el caso de la RIP Act (RIPA) en Reino Unido con respecto a la USA Patriot Act en Estados Unidos. Ver GRINGAS, C. UK Cloud Computing Interception - nothing new. *Olswang*. 2011. Disponible en web: http://www.olswang.com/pdfs/CloudComputingInterception_CQG.pdf.

[857] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 05/2012 sobre la computación en nube. Ob. cit. p. 7.

[858] PARLAMENTO EUROPEO. Resolución del Parlamento Europeo, de 10 de diciembre de 2013, sobre la liberación del potencial de la computación en la nube en Europa. 10 de diciembre de 2013. Disponible en web: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0535+0+DOC+XML+V0//ES

[859] Acceso al texto de la norma en el siguiente enlace: http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf
Un buen resumen de la norma, en el trabajo realizado por la BBC. UK surveillance powers explained. November 5th, 2015. Disponible en web: http://www.bbc.com/news/uk-34713435

entreguen la llave de encriptado, aunque esta obligación no se puede imponer respecto a compañías extranjeras. Ciertamente se establece un cierto control judicial para evitar abusos como por ejemplo el sistema de "doble llave" en las órdenes de interceptación de tal modo que cuando un ministro lo autorice, la orden no se pone en marcha hasta que los comisionados den la autorización, a quienes corresponde también la inspección de los trabajos secretos del MI5 y otras agencias. Efectivamente el control se hace recaer en un Nuevo órgano de comisionados, encabezado por el Comisionados de Poderes de Investigación (IPC en su acrónimo inglés) al que corresponderá la supervisión de todos los poderes de investigación. En todo caso, se trata de una norma que nace ya con polémica por cuanto el pasado 21 de diciembre de 2016[860] el TJUE declaró nula la conocida como DRIPA[861], norma que autorizaba en el Reino Unido la posibilidad de recogida masiva de correos electrónicos y otros datos de los ciudadanos, aunque admite la retención dirigida de datos solamente por razones de lucha contra crímenes graves y en lo estrictamente necesario.

En definitiva y como primera conclusión, coincidimos con el profesor Walden cuando señala que los miedos actuales respecto a los proveedores de servicios cloud americanos son más una consecuencia de su actual dominio en el mercado mundial, mientras que las preocupaciones sobre el alcance potencial de los agentes de la autoridad, particularmente mediante la conocida como "Patriot Act" reflejan una ignorancia generalizada respecto al poder de que gozan otras agencias gubernamentales en muchas, si no en la mayoría de las jurisdicciones más avanzadas[862].

Existen un conjunto de normas que han venido regulando el acceso por parte de las autoridades norteamericanas[863] a los datos[864]:

---

[860] Unión Europea. Tribunal de Justicia de la Unión Europea. Caso Tele2 Sverige AB v Post-ochtelestyrelsen (C-203/15) y Secretary of State for the Home Department vs Tom Watson and Others (C-698/15). Sentencia de 21 de diciembre de 2016. El texto de la Sentencia no se encuentra todavía disponible en el momento de redactar estas líneas. El acceso al resumen de prensa en siguiente enlace: thttp://curia.europa.eu/jcms/upload/docs/application/pdf/2016-12/cp160145en.pdf

[861] *Data Retention and Investigatory Powers Act* aprobada en 2014 y a cuyo texto original se puede acceder en el siguiente enlace: http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf

[862] WALDEN, I. ob. Cit.

[863] IT LAW GROUP. USA Patriot Act Effect on Cloud Computing Services. Disponible en web: http://www.itlawgroup.com/resources/articles/113-usa-patriot-act-effect-on-cloud-computing-services

[864] La cuarta enmienda a la Constitución de los Estados Unidos recoge: "El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas".

NORMAS QUE RIGEN EL ACCESO POR PARTE DE LAS AUTORIDADES DE EE.UU. A LOS DATOS EN LA NUBE

Fuente: elaboración propia

Sea por uno u otro motivo, lo cierto es que la polémica en torno a los proveedores de servicios americanos existe. Por ello nos corresponde adentrarnos, por su trascendencia, en el tratamiento que de esta cuestión se hace en el acuerdo existente entre la Comisión Europea y el Departamento de Comercio de los Estados Unidos y que hoy día se encuentra plasmado en el denominado Escudo de Privacidad.

Efectivamente, en este acuerdo, el acceso a datos por las autoridades públicas ha sido una de las cuestiones más sensibles como consecuencia de la citada normativa estadounidense. Ya en sendas Comunicaciones de 2013[865], la Comisión Europea señalaba la necesidad de revisar y fortalecer las bases fundamentales del esquema de Acuerdo Seguro en el contexto

[865] EUROPEAN COMMISSION. Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EUU.S. Data Flows, COM (2013) 846 final, 27 de noviembre de 2013. Disponible en web: http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf
EUROPEAN COMMISSION. Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies established in the EU, COM(2013) 847 final, 27 de noviembre de 2013 Disponible en web: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf

de un número de factores, incluyendo: el crecimiento exponencial de los flujos de datos y su importancia crítica para la economía trasatlántica, el rápido crecimiento del número de empresas americanas que se adherían a dicho esquema y, a los efectos que nos ocupan, la nueva información en cuanto a la escala y el ámbito de determinados programas de inteligencia que planteaban preguntas en cuanto al nivel de protección que podía garantizar. Además subrayaba aspectos como que la reforma de la normativa de protección de datos "incluye normas claras respecto a las obligaciones y responsabilidades de los encargados del tratamiento como los proveedores *cloud*, incluyendo la seguridad". Y añadía "como han demostrado las revelaciones respecto a los programas de inteligencia, esto es algo crítico porque afecta a datos almacenados en la nube. También, las empresas que facilitan espacios de almacenamiento en la nube que son requeridos para facilitar datos personales a autoridades extranjeras no serán capaces de evadir su responsabilidad alegando su condición de encargados en lugar de responsables"[866].

En la misma línea, el Parlamento Europeo manifestaba su gran preocupación por una doble vertiente de acceso que tienen en ambos casos impacto directo en la nube: por un lado, la divulgación directa y obligatoria de información y datos personales de la UE, tratados con arreglo a contratos de servicios en la nube, a autoridades de terceros países por los prestadores sujetos a la legislación de un tercer país o que utilizan servidores de almacenamiento ubicados en terceros países; y en segundo lugar, por el acceso directo a distancia a los datos e información personales tratados por autoridades policiales y servicios de inteligencia de terceros países[867].

A todo ello se añaden las consecuencias derivadas del caso *Schrems*[868]*.* El caso trae causa de cuando el 25 de junio de 2013 el Sr. Schrems presentó ante el comisario una reclamación en la que le solicitaba en sustancia que ejerciera sus competencias estatutarias, prohibiendo a Facebook Ireland transferir sus datos personales a Estados Unidos. Alegaba que el

[866] EUROPEAN COMMISSION. Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EUU.S. Data Flows. Ob. cit. p. 6. Disponible en web: http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf

[867] PARLAMENTO EUROPEO. Resolución del Parlamento Europeo, de 10 de diciembre de 2013, sobre la liberación del potencial de la computación en la nube en Europa", 10 de diciembre de 2013, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0535+0+DOC+XML+V0//ES

[868] Unión Europea. Tribunal de Justicia de la Unión Europea. Caso *Schrems* (C-362/14). Sentencia de 6 de octubre de 2015 Acceso al texto de la Sentencia en el siguiente enlace: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5a84598616c2946f5a4edcb4c9876014b.e34KaxiLc3eQc40LaxqMbN4Pah0Re0?text=&docid=169195&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=197646

Derecho y las prácticas en vigor en este último país no garantizaban una protección suficiente de los datos personales conservados en su territorio contra las actividades de vigilancia practicadas en él por las autoridades públicas. El Sr. Schrems hacía referencia en ese sentido a las revelaciones del Sr. Edward Snowden sobre las actividades de los servicios de información de Estados Unidos, en particular las de la National Security Agency (en lo sucesivo, «NSA»). La *High Court* irlandesa (por razones de domicilio social de Facebook en este caso), tras recordar que "el acceso masivo e indiferenciado a los datos personales es manifiestamente contrario al principio de proporcionalidad y a los valores fundamentales protegidos por la Constitución irlandesa", señaló, en el planteamiento de la cuestión prejudicial, que "el derecho al respeto de la vida privada garantizado por el artículo 7 de la Carta y por los valores esenciales comunes a las tradiciones de los Estados miembros quedaría privado de alcance alguno si se permitiera a los poderes públicos acceder a las comunicaciones electrónicas de manera aleatoria y generalizada, sin ninguna justificación objetiva fundada en razones de seguridad nacional o de prevención de la delincuencia ligadas específicamente a los individuos afectados, y sin que esas prácticas se rodeen de garantías adecuadas y comprobables".

Pues bien, uno de los elementos que sirvió al Tribunal de Justicia de la Unión Europea en el caso *Schrems* para anular el Acuerdo de Puerto Seguro, era precisamente que "la Decisión 2000/520 no contiene ninguna constatación sobre la existencia en Estados Unidos de reglas estatales destinadas a limitar las posibles injerencias en los derechos fundamentales de las personas cuyos datos se transfieran desde la Unión a Estados Unidos, injerencias que estuvieran autorizadas a llevar a cabo entidades estatales de ese país cuando persigan fines legítimos, como la seguridad nacional". Las excepciones a los principios del acuerdo de puerto seguro podían limitarse cuanto sea necesario para cumplir las exigencias de seguridad nacional, interés público y cumplimiento de la ley[869]. Pero como concluye la Sentencia, "No se limita a lo estrictamente necesario una normativa que autoriza de forma generalizada la conservación de la totalidad de los datos personales de todas las personas cuyos datos se hayan transferido desde la Unión a Estados Unidos, sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin prever ningún

[869] COMISIÓN EUROPEA. 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 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. Disponible en web: http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/common/B.12-cp--Decisi-oo-n--sobre-la-adecuaci-oo-n-conferida-por-los-principios-de-puerto-seguro.pdf

criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización".

El nuevo Escudo de Privacidad pretende dar respuesta a estas necesidades.

Fuente: elaboración propia

Una de las partes clave y que merece un apartado específico es el que lleva por rúbrica "Acceso a los datos personales transferidos en el marco del Escudo de la privacidad UE-EE.UU. y utilización de los mismos por los poderes públicos estadounidenses". Se lleva a cabo una minuciosa descripción de la normativa de los Estados Unidos que permite la posibilidad de acceder a los datos de ciudadanos de la Unión Europea por parte de las autoridades estadounidenses.

La Comisión Europea ha resumido[870] las características del Escudo de Privacidad que en este punto en concreto viene a señalar tanto los condicionantes para que esto se produzca, como los fundamentales mecanismos de supervisión y de control, donde existen mayores novedades. Se subraya como aspecto más relevante que "Por primera vez, los Estados Unidos han concedido a la UE sólidas garantías de que el acceso de las autoridades públicas encargadas de los servicios coercitivos y de la seguridad nacional estará sujeto a limitaciones, salvaguardas y mecanismos de supervisión claros. Estas excepciones deben utilizarse únicamente en la medida de lo necesario y de forma proporcionada. Los EE.UU. han descartado la vigilancia masiva indiscriminada de los datos personales transferidos a los EE.UU. en el marco del nuevo mecanismo. A fin de supervisar regularmente el funcionamiento del mecanismo habrá una revisión conjunta anual, que también incluirá la cuestión del acceso de la seguridad nacional. La Comisión Europea y el Departamento de Comercio de los EE.UU. llevarán a cabo la revisión e invitarán a la misma a expertos de los servicios de inteligencia de los EE.UU. y de las autoridades europeas de protección de datos"[871]. En lo que se refiere a los condicionantes es necesario descender al contenido de la Decisión propiamente dicha[872] y más concretamente a los puntos 64 y siguientes. Como decimos y de manera resumida podemos subrayar:

A) la PPD-28[873], adoptada el 17 de enero de 2014, impone una serie de limitaciones a las operaciones de "inteligencia de señales": se podrá recabar exclusivamente a efectos de inteligencia exterior o contrainteligencia para apoyar misiones nacionales y ministeriales, y se prioriza la recopilación selectiva frente a la recopilación indiscriminada. Además, aunque los Estados Unidos consideren necesaria la recopilación indiscriminada de inteligencia de señales, la referida directiva presidencial 28 limita el uso de dicha información a una lista específica de seis fines

[870] COMISIÓN EUROPEA. Guía acerca del Escudo de Privacidad UE-EE.UU. 2016. Disponible en web: https://www.agpd.es/portalwebAGPD/noticias-inicio/common/pdf/2016/08_agosto/es_56972_citizens-guide_en.pdf

[871] COMISIÓN EUROPEA. Nota de Prensa de 2 de febrero de 2016, "La Comisión Europea y los Estados Unidos acuerdan un nuevo marco para los flujos transatlánticos de datos: Escudo de la privacidad UE - EE.UU", http://europa.eu/rapid/press-release_IP-16-216_es.htm

[872] COMISIÓN EUROPEA. Decisión de Ejecución de la Comisión con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU", 12 de julio de 2016, http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2016/07-11/C_2016_4176_F1_COMMISSION_IMPLEMENTING_DECISION_ES.pdf

[873] *Presidential Policy Directive 28, "Signals Intelligence Activities"*, 17 de enero de 2014, https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

de seguridad nacional: el espionaje, el terrorismo, las armas de destrucción masiva y las amenazas de ciberseguridad para las Fuerzas Armadas o el personal militar, así como las amenazas delictivas transnacionales relacionadas con los otros cinco fines.

Como se recoge en el punto 76 de la Decisión de la Comisión Europea, por cierto, redactado con un cierto tono justificativo que llama la atención, "aunque no se formule en tales términos jurídicos, estos principios captan la esencia de los principios de necesidad y proporcionalidad. Se concede una clara prioridad a la recopilación selectiva, mientras que la recopilación indiscriminada se limita a situaciones (excepcionales) en las que no es posible llevar a cabo una selectiva por motivos técnicos u operativos. Aun cuando no pueda evitarse la recopilación indiscriminada, el acceso a tales datos y su posterior utilización se limita estrictamente a fines legítimos y específicos de seguridad nacional".

El problema, como todo lo conceptual, es la indeterminación a que pueden dar lugar algunos de esos términos. A pesar de las garantas otorgadas, la investigación de algunos de esos delitos que amparan supuestos de vigilancia masiva, están llamados a crear nuevos problemas. El equilibrio de nuevo que hemos apuntado al principio entre privacidad y seguridad, o entre esta y la libertad, pueden quebrar dependiendo de la concreción de conductas que se ubiquen bajo cada uno de estos conceptos. Los mecanismos de evaluación y supervisión conjuntos que están llamados a ponerse en marcha y la mayor o menor concreción de los mismos serán un botón de muestra de hasta qué punto resulta adecuado este nuevo marco de cooperación.

B) Una vez que los datos se hayan transferido a entidades ubicadas en los Estados Unidos y autocertificadas en el marco del Escudo, los servicios de inteligencia estadounidenses solo podrán recabar datos personales si su petición cumple la Ley de Vigilancia de Inteligencia Exterior[874]; o procede del FBI, sobre la base de una denominada Carta de Seguridad Nacional. Dichas bases jurídicas sin embargo tienen limitadas las posibilidades de vigilancia indiscriminada, por cuanto la Ley de Libertad de los Estados Unidos[875], aprobada el 2 de junio de 2015, fundamentalmente prohíbe la recopilación indiscriminada y exige términos de selección.

[874] Acceso al texto de la norma en el siguiente enlace: https://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf
[875] Acceso al texto de la norma en el siguiente enlace: https://www.congress.gov/114/bills/hr2048/BILLS-114hr2048enr.pdf

Otra vertiente relevante, y de mucha implicación para el *cloud* y para los clientes que alojen datos de ciudadanos europeos en servidores de empresas estadounidenses, es cuando dichos datos se encuentren alojados en territorio europeo, en virtud de la cláusula europea que tan frecuente resulta en la prestación de este tipo de servicios. Lo normal es que cuando sea necesario conocer esos datos, se recurra a los mecanismos de cooperación internacional ya existentes, como los tratados de asistencia jurídica mutua (MTAS en sus siglas inglesas[876]), criterio por el que se inclina de hecho la industria de una manera preferente[877].

En el campo que nos ocupa, pensemos por ejemplo en el Capítulo III del Convenio sobre la Ciberdelincuencia, que contempla un conjunto de medidas en el ámbito de la cooperación internacional, entre las que se encuentra el artículo 23.1 que nos dice que "Las Partes cooperarán entre sí en la mayor medida posible, de conformidad con las disposiciones del presente capítulo, en aplicación de los instrumentos internacionales aplicables a la cooperación internacional en materia penal, de acuerdos basados en legislación uniforme o recíproca y de su derecho interno, para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos".

Sin embargo, más allá del *desiderátum*, resulta cierto que en determinadas ocasiones las autoridades pueden intentar obtener la información haciendo el requerimiento a la filial americana de una empresa ubicada en el exterior que puede tener custodia o control sobre los documentos o información en juego. Los tribunales americanos, a raíz del caso del Banco

---

[876] Es el caso por ejemplo de Alemania que firmó un acuerdo de asistencia jurídica mutua en materia penal con los Estados Unidos en 2003 y otro complementario en 2006. Ambos tratados, hoy día en vigor, permiten a las autoridades de cada país requerir y recibir información ubicada en otras jurisdicciones (incluyendo información almacenada en infraestructuras de terceros). Ver MAXWELL, W. y WOLF, F.CH. A Global Reality: Governmental Access to Data in the Cloud A comparative analysis of ten international jurisdictions. *A Hogan Lovells White Paper*. Disponible en web: http://www-05.ibm.com/ch/services/documents/sce/br-government-access-to-cloud-data.pdf

[877] DIGITAL EUROPE. Law Enforcement Access to Data in the European Cloud. Disponible en web: http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=849&language=en-US&PortalId=0&TabId=353

En la misma línea se pronunció Kim Gagne, Director Senior de Relaciones Institucionales de Microsoft, Fundación para la Investigación sobre el Derecho y la Empresa, "Jornadas sobre Acceso legítimo de autoridades a datos personales almacenados en el extranjero y los mecanismos de cooperación internacional", 29 de marzo de 2016, http://www.fidefundacion.es/Acceso-legitimo-de-autoridades-a-datos-personales-almacenados-en-el-extranjero-y-los-mecanismos-de-cooperacion_a292.html

Nova Scotia[878], han venido aplicando una doctrina en virtud de la cual una empresa con presencia en Estados Unidos está obligada a responder a una demanda de información valida por parte del Gobierno americano y bajo leyes americanas siempre que la empresa tenga custodia o control sobre los datos. La clave siempre está en saber si la compañía americana tiene la referida custodia o control. Cabe reseñar que esta misma doctrina se ha aplicado en otros países en el caso por ejemplo del Banco de Valeta en Australia[879].

Sin embargo, se trata de una doctrina que a día de hoy tiene matices y para muestra, un botón[880]. Uno de los supuestos de mayor repercusión en este ámbito fue un conocido caso de la compañía Microsoft en el que se produjo un vaivén judicial en diferentes instancias respecto a la posibilidad por parte de las autoridades norteamericanas de exigir el acceso a los datos de un servidor ubicado en Irlanda[881]. El caso comenzó cuando un juez magistrado federal en Nueva York en noviembre de 2013 autorizó una orden de registro como parte de una investigación criminal. A mediados de 2014 Microsoft recurrió dicha orden cuestionando si unos fiscales federales podían obligar a entregar las comunicaciones de mail de un cliente almacenadas en un centro de datos en Irlanda. Se trataba de la primera vez que una empresa se oponía a una orden de registro de información digital en el extranjero. Prueba de su importancia es el conjunto de escritos *amicus curiae*[882] que presentaron un conjunto de compañías y otras organizaciones[883].

---

[878] Tribunal de Apelación del Undécimo Circuito. Caso Banco Nova Scotia. Sentencia de 14 de agosto de 1984. Acceso al texto de la Sentencia en el siguiente enlace: http://law.justia.com/cases/federal/appellate-courts/F2/740/817/233788/

[879] Australia. Tribunal Federal. *Caso Bank of Valletta PLC vs National Crime Authority*. Sentencia de 13 de agosto de 1999. Acceso al texto de la Sentencia en el siguiente enlace: https://jade.io/article/117281

[880] En la estela de las filtraciones de Edward Snowden a mediados de 2013, los clientes comerciales europeos presionaron a los proveedores de nube americanos para explicar cómo prevenían el acceso por las agencias de inteligencia americanas u otras autoridades. Varios proveedores, incluyendo Microsoft, desarrollaron soluciones de "nube europea". Sin embargo, los competidores europeos, citando los casos de la doctrina *Bank of Nova Scotia*, argumentaron que los datos almacenados en cualquier sitio por un proveedor americano podrían ser obtenidos potencialmente por las autoridades americanas. El hecho de que Microsoft recibiera una orden de registro para un correo no americano en la estela de las filtraciones de Snowden dio lugar, en parte a la petición de la compañía para que fuera anulada. McGRAW SWAMINATHA, T. y NEFF, K. Microsoft-Ireland: Decision underscores tension between privacy principles and the digital environment. *DLA Pipper*. 19 de junio de 2016. Disponible en web: https://www.dlapiper.com/en/us/insights/publications/2016/07/microsoft-v-us-decision-underscores-tension/

[881] Relato de los hechos tomado de WINGFIELD, N. y KANG, C. Microsoft Wins Appeal on Overseas Data Search. *New York Times*. 14 de julio de 2016. Disponible en web: http://www.nytimes.com/2016/07/15/technology/microsoft-wins-appeal-on-overseas-data-searches.html?_r=0

[882] Término con el que se conoce el escrito que dirige al tribunal alguien interesado en el objeto del litigio pero que no forma parte del mismo.

[883] *Apple, Amazon, Verizon Communications, Fox News, National Public Radio, The Washington Post, CNN* y casi dos docenas más de empresas de comunicación y tecnológicas; sindicatos, grupos de *advocacy*,

En 2014, el Juez James Francis, Magistrado de la Corte de Distrito para el Distrito Sudeste de Nueva York, se posicionó con el Gobierno diciendo que la orden para desvelar los correos electrónicos almacenados en Irlanda "no era una orden convencional, sino más bien, la orden era un híbrido: parte una orden de registro y parte una citación *(subpoena*)". Se dicta como una orden, con un juez considerando como probable que los documentos requeridos podrían dar evidencias de delito, pero que se ejecuta como una citación, por cuanto se dicta directamente a la compañía y no implica a agentes federales entrando y buscando en los servidores de la compañía y añadía que "está jurídicamente reconocido que una citación exige a su receptor para que facilite la información en su posesión…con independencia de la ubicación de dicha información".

En julio de 2016, la Corte de Apelación para el Segundo Circuito[884] señalaba que, "en 1986, cuando el Congreso aprobó la Ley de Comunicaciones Almacenadas (*Stored Communications Act*) como una parte de la Ley de Privacidad en las Comunicaciones Electrónicas (*Electronic Communications Privacy Act*) tenía como objetivo proteger la privacidad de los usuarios en el contexto de una nueva tecnología que exigía de la interacción del usuario con el proveedor del servicio. Ni explícita ni implícitamente la norma prevé la aplicación de sus previsiones de órdenes en el extranjero. Hace tres décadas, las fronteras internacionales no se cruzaban de manera tan rutinaria como hoy día, cuando los proveedores de servicios descansan en redes de *hardware* a lo largo y ancho del mundo para satisfacer las demandas de los usuarios del siglo XXI en cuanto a acceso y velocidad y todo lo relacionado, incluyendo expectativas de privacidad".

Esta jurisprudencia se ha visto cuestionada más recientemente, si bien por vía de un tribunal de primera instancia. En concreto, el pasado 3 de febrero de 2017[885], el juez de distrito para el distrito este de Pennsylvania, se enfrentaba a un supuesto en el que se habían dictado dos órdenes judiciales al amparo de la Ley de Comunicaciones Almacenadas solicitando el acceso al contenido de correos electrónicos. Google respondió con los correos que sabía estaban almacenados en Estados Unidos, pero se negó respecto a los almacenados fuera

incluyendo la Unión Americana de Libertades Civiles y la Cámara de Comercio de Estados Unidos, así como 35 informáticos.

[884] Estados Unidos. Corte de Apelación del Segundo Circuito. *Caso Microsoft vs Estados Unidos.* Sentencia de 14 de julio de 2016. Acceso al texto completo de la Sentencia en el siguiente enlace: http://digitalconstitution.com/wp-content/uploads/2016/07/Decision-opinion.pdf

[885] Estados Unidos. Tribunal de Distrito para el Distrito Este de Pennsylvania. Sentencia de 3 de febrero de 2017. Acceso al texto de la Sentencia en el siguiente enlace: https://www.washingtonpost.com/news/volokh-conspiracy/wp-content/uploads/sites/14/2017/02/Opinion.pdf?tid=a_inl

apelando a la doctrina Microsoft. El principal argumento utilizado por el Magistrado Thomas J. Reuter para obligar a Google fue que la "conducta relevante para la SCA (*Stored Communications Act*) tendría lugar en Estados Unidos incluso para los datos recuperados de fuera de Estados Unidos. La invasión de privacidad tendría lugar en Estados Unidos; el registro de los datos electrónicos revelados por Google tras el mandato judicial ocurriría en Estados Unidos cuando el FBI revisara las copias de los datos requeridos en Pennsylvania y consiguientemente estaríamos ante una permitida aplicación doméstica de la SCA.

Sin perjuicio de que habrá que esperar a lo que en apelación se resuelva, sí que es claro que la doctrina del caso Microsoft, que se vuelve a posicionar de manera favorable a los mecanismos de cooperación internacional frente a los de actuación unilateral, se ha venido a recoger en gran medida en el RGPD en lo que se ha venido en llamar la cláusula anti-FISA. En concreto se trata del artículo 48 que lleva por rúbrica "Transferencias o comunicaciones no autorizadas por el Derecho de la Unión" y que señala que cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro, sin perjuicio de otros motivos para la transferencia al amparo del presente capítulo". Se trata de una cláusula que fue incluida por el Parlamento Europeo, vía enmienda, a raíz de los escándalos del caso Snowden y que por ejemplo el Reino Unido no considera aplicable[886] y que no es nueva por cuanto ya había sido defendida por la institución parlamentaria con anterioridad[887].

También en el plano normativo el Consejo de Europa ha explicado a través de una guía interpretativa lo que se puede y no se puede hacer bajo el paraguas del artículo 32 de la

---

[886] Así se puede observar en el pronunciamiento del Gobierno británico: http://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Lords/2016-02-04/HLWS500/
Se trata de una postura basada en el Protocolo 21 al Tratado de Funcionamiento de la Unión Europea (sobre la posición del reino Unido en las áreas de libertad, seguridad y justicia) y que responde a un sistema opt-in, es decir, es el Reino Unido el que tendría que manifestarse expresamente respecto a verse vinculado por dicha previsión.

[887] En su Resolución de 2013 ya citada, el Parlamento Europeo deploraba que el acceso suela hacerse por medio de la aplicación directa por parte de las autoridades de terceros países de sus propias normas jurídicas sin utilizar instrumentos internacionales de cooperación judicial, como la asistencia judicial mutua u otras formas de cooperación judicial. PARLAMENTO EUROPEO. Resolución del Parlamento Europeo, de 10 de diciembre de 2013, sobre la liberación del potencial de la computación en la nube en Europa. 10 de diciembre de 2013, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0535+0+DOC+XML+V0//ES

Convención sobre Cibercriminalidad. Recordemos que este precepto contempla dos supuestos que quedan reflejados en su propia rúbrica: "Acceso transfronterizo a datos almacenados, con consentimiento o cuando estén a disposición del público". Por un lado, se señala que una Parte (un Estado en definitiva), sin la autorización de otra podrá tener acceso a datos informáticos almacenados que se encuentren a disposición del público (fuente abierta), con independencia de la ubicación geográfica de dichos datos. En este supuesto, marcado por la sencillez y de menor trascendencia para lo que nos ocupa, el Subgrupo de Acceso Transfronterizo y Jurisdicción señaló que es comúnmente aceptado que los agentes de la autoridad puedan acceder a los datos que el público puede acceder y que para ello pueden darse de alta o registrarse en servicios accesibles al público, aunque reconoce que algunas normas nacionales establecen determinados límites. Igualmente añade que, si una porción de la información está cerrada al público, no se puede considerar como pública a efectos del referido precepto. El segundo de los supuestos, de mayor trascendencia a nuestros efectos, es el que permite a un Estado, sin autorización de otro, esto es, sin necesidad de un tratado distinto del de la propia convención, tener acceso o recibir, a través de un sistema informático situado en su territorio, datos almacenados en otro Estado, si se obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada para revelar los datos por medio de ese sistema informático. En este caso sin embargo la guía de interpretación del mencionado subgrupo establece una serie de condiciones a tener en cuenta que quedan resumidas, en lo más relevante, en la siguiente figura[888]:

[888] *Ad-hoc Subgroup on Transborder Access and Jurisdiction, "Transborder access to data and jurisdiction: Options for further action by the T-CY"*, 2 de diciembre de 2014, páginas 18 y siguientes, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pdf
La adopción del informe final respecto a esta interpretación del artículo 32 a cargo del Comité de la Convención sobre Cibercriminalidad estaba previsto, en el calendario original, que se adoptara en diciembre de 2016. Ob. cit, página 21.

Consideraciones generales
• Se aplica a procedimientos e investigaciones criminales específicas en el ámbito de aplicación de la Convención. •El Estado podrá considerar notificar al Estado en que se encuentren alojados los datos.
Concepto de transfronterizo y ubicación
•Transfronterizo significa "acceso unilateral a datos informáticos almacenados en otro Estado sin requerir asistencia mutua". •Solo resulta aplicable cuando se sabe dónde están alojados los datos y no cubre cuando no estén almacenados en otro Estado parte en la Convención o cuando no se tenga certeza de su ubicación.
Concepto de consentimiento
•El consentimiento lícito y voluntario significa que la persona que facilite el acceso o la revelación de los datos no puede ser obligada o engañado. •En la mayoría de los Estados la cooperación en investigacione penales requerirá un consentimiento explícito y por ejemplo el consentimiento de una persona a los términos y ondiciones de uso podrá no equipararse a un consetimiento explícito.
Persona que puede dar acceso
•puede ser una persona física, permitiendo el acceso a su cuenta de correo o a otros datos alojados en el extranjero. •puedes ser también una perona jurídica •en cuanto a los proveedores de servicios no están autorizados a dar un consentimiento válido y voluntario para permitir el acceso a los datos de sus clientes. Normalente solo serán poseedores de esos datos yno los controlarán ni serán de su propiedad y consiguientemente no podrán otorgar consentimientos. en etos casos será necesarios otros métidos como la asistencia jurídica mutua o procedimientos para situaciones de emergencia.

Fuente: elaboración propia

3.4 La situación en España tras la reforma procesal

Como no podía ser de otro modo, también en la normativa española se ha afrontado esta cuestión que, insistimos, no es exclusiva de los proveedores americanos. Desde el punto de vista normativo, a título de ejemplo, en España la posibilidad por parte de las Fuerzas y Cuerpos de Seguridad del Estado de acceder a los datos se recoge por dos vías. Por un lado, de manera directa, teniendo en cuenta que el artículo 22 LOPD que señala que la recogida y tratamiento para fines policiales sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales; y añade que en el caso de datos especialmente protegidos podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

En todo caso, para esta habilitación directa, la Agencia Española de Protección de Datos exige que concurran una serie de circunstancias[889]: a) Que quede debidamente acreditado que la obtención de los datos resulta necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales y que, tratándose de datos especialmente protegidos, sean absolutamente necesarios para los fines de una investigación concreta. b) Que se trate de una petición concreta y específica, al no ser compatible con lo señalado anteriormente el ejercicio de solicitudes masivas de datos. c) Que la petición se efectúe con la debida motivación, que acredite su relación con los supuestos que se han expuesto. d) Que, en cumplimiento del artículo 22.4 de la Ley Orgánica 15/1999, los datos sean cancelados "cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento".

Por otro lado, también cabe la posibilidad de cesión de manera indirecta, que tiene mayor repercusión en nuestro caso, en el que se dice que la cesión de datos no requerirá el consentimiento cuando la cesión está autorizada en una ley o cuando la comunicación que deba efectuarse tenga por destinatario, al Ministerio Fiscal o los Jueces o Tribunales, ubicando en esta categoría a la policía judicial, siempre y cuando exista mandamiento judicial o requerimiento del Ministerio Fiscal que dé cobertura a la cesión[890].

Especial referencia por su carácter reciente hay que hacer a la reforma introducida en el año 2015 en el ámbito procesal penal. Como señala Tejada de la Fuente, la insuficiencia normativa hasta ahora "ha sido paliada en buena medida con la valiosa y consolidada doctrina elaborada en los últimos años por nuestros Tribunales, tanto Tribunal Supremo como Tribunal Constitucional, sobre las garantías y formalidades con que debe llevarse a efecto cualquier diligencia de investigación que afecte a derechos fundamentales. Esta doctrina, construida a partir de los preceptos de nuestra añeja norma procesal, ha hecho posible extender su alcance a las situaciones que actualmente se han de abordar -en ocasiones muy diferentes a aquellas para las que fueron elaborados- preservando en todo caso los principios y valores que constituyen el fundamento de nuestro sistema jurídico"[891].

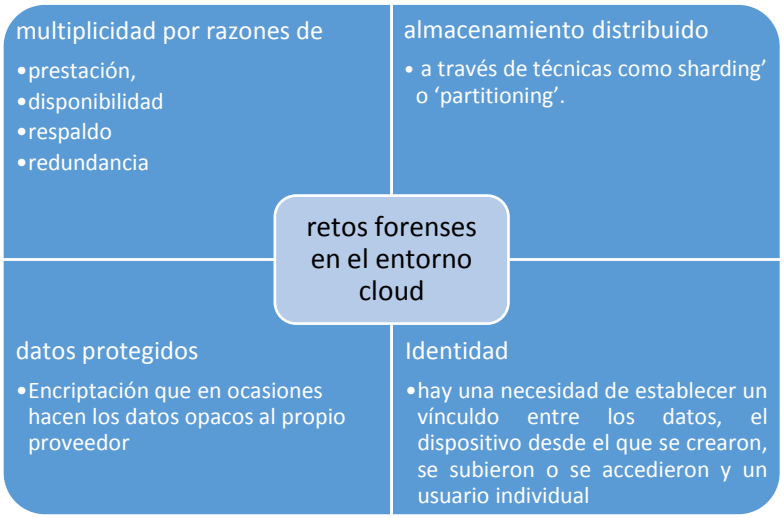
---

[889] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Informe 0133/2008. Disponible en web: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2008-0133_Comunicacion-de-datos-a-la-Policia-Judicial-sin-mandamiento-judicial.pdf

[890] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Procedimiento 00551/2011. Disponible en web: http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2012/common/pdfs/PS-00551-2011_Resolucion-de-fecha-22-05-2012_Art-ii-culo-4.3-LOPD_Recurrida.pdf

[891] TEJADA DE LA FUENTE, E. Apuntes sobre la reforma procesal en materia de investigación tecnológica. *Revista de Privacidad y Derecho Digital.* Abril 2016. Nº 3. p. 181-190.

La reforma incluye un conjunto de medidas de investigación tecnológica. Se trata de una cuestión fundamental, y máxime si tenemos en cuenta que de por sí ya existen otros problemas prácticos, como son los retos forenses a los que se enfrenta la obtención de evidencias en el entorno cloud y que se concretan en cuatro aspectos recogidos en la siguiente figura:



Fuente: elaboración propia con base en artículo de Walden

Se trata de lo que muy gráficamente Cabezudo Rodríguez ha denominado el lado perverso de la revolución tecnológica[892]. Este mismo autor recuerda que la obtención de elementos probatorios situados fuera del territorio del Estado interesado puede chocar con intereses nacionales legítimos (defensa de la soberanía) o, menos legítimos (paraísos de impunidad tecnológica); y añade que esa extraterritorialidad de las pruebas puede devenir en su total deslocalización cuando se trate de archivos o programas alojados en «La Nube».

Sin entrar en el detalle de la reforma procesal, cabe destacar dos puntos concretos por su particular aplicabilidad al *cloud computing*: el registro de dispositivos de almacenamiento masivo y el acceso remoto a contenidos en sistemas informáticos.

[892] CABEZUDO RODRÍGUEZ, N. Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal. en AA.VV. *I Jornada del Boletín del Ministerio de Justicia: «Las reformas del proceso penal»*. Febrero de 2016 Año LXX. Núm. 2186. p. 6 y siguientes,

Previamente a tratar cómo ha quedado dicha reforma finalmente, merece la pena detenerse, siquiera con una sucinta referencia, en el Proyecto de Código Procesal Penal previo, ya que recogía alguna disposición de enorme interés para lo que estamos tratando, y muy concretamente si tenemos en mente el caso *Microsoft* al que antes hemos hecho mención. En concreto, merece destacarse el apartado cuarto del art. 350 de dicho texto[893], que establecía que el registro remoto sólo podía ser autorizado cuando los datos se encontraran almacenados en un sistema informático *o en una parte del mismo situado en territorio sobre el que se extienda la jurisdicción española* (la cursiva es nuestra). En otro caso, se debía recurrir a las medidas de cooperación judicial internacional en los términos establecidos por la Ley, los Tratados y Convenios internacionales aplicables y el derecho de la Unión Europea.

Pero más interés si cabe tienen las reflexiones que realizaba el Ministerio Fiscal en el Informe emitido por el Consejo Fiscal al Anteproyecto de Ley Orgánica de Modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas, en el que se recogía un apartado específico referido al acceso a contenidos almacenados en la nube[894]. En dicho Informe subrayaba, y esto es lo que más nos interesa, que a la vista de las enormes dificultades para ubicar físicamente dónde se encuentran los archivos en los supuestos de utilización de la nube, debiera preverse la posibilidad de que el acceso a información contenida en sistemas de *cloud computing* se autorizara por las autoridades judiciales españolas siempre que nuestros tribunales fueran competentes para conocer de la causa que se está investigando. Pero a mayor abundamiento, y en una reflexión que va directamente a la esencia de Internet en sí misma y de la nube en concreto, se argumentaba por parte del máximo organismo del Ministerio público, que "en tanto en cuanto se tiene acceso al material desde España por un imputado situado en nuestro territorio, el mismo se posee en España, y, consiguientemente, las autoridades españolas tendrían jurisdicción para acceder al mismo". Sin duda esta idea resulta sumamente útil a efectos de la labor investigadora, recurriendo a un punto de conexión de mera jurisdicción, aunque plantea

---

[893] Acceso al texto del Proyecto de Código Procesal Penal en el siguiente enlace: http://www.mjusticia.gob.es/cs/Satellite/Portal/1292375190463?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadername2=Medios&blobheadervalue1=attachment%3B+filename%3DCODIGO_PROCESAL_PENAL.pdf&blobheadervalue2=1288778173060

[894] CONSEJO FISCAL. Informe emitido por el Consejo Fiscal al Anteproyecto de Ley Orgánica de Modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas. 23 de enero de 2015. Disponible en web: http://pdfs.wke.es/2/2/7/8/pd0000102278.pdf

dudas por los conflictos de soberanía que pudiera acarrear, lo que finalmente nos lleva, de nuevo a los tratados de asistencia jurídica mutua.

La regulación que finalmente se ha recogido en la Ley de Enjuiciamiento Criminal no ha contemplado esta interesante reflexión en el plano geográfico y plantea dudas desde el punto de vista de su aplicabilidad práctica en aquellos casos en que los datos se encuentren alojados fuera del territorio español. La medida que tiene una naturaleza muy invasora, así como la redacción original y la redacción actual, invitan a pensar que la solicitud de la fiscalía no resulta aplicable en este caso.

Sin entrar en los detalles de la reforma sí que cabe subrayar los dos supuestos que hemos mencionado pueden impactar en la computación en nube: el registro de dispositivos de almacenamiento masivo y el acceso remoto. Mencionar que lo delicado de la materia, su afectación a los derechos fundamentales y la naturaleza invasora en el párrafo anterior han hecho que la regulación sea particularmente estricta y rodeada de garantías en ambos supuestos.

En el caso del registro de dispositivos de almacenamiento masivo de información, regulado en los artículos 588 sexies de la LECrim, se exige, por un lado que la resolución del juez de instrucción será la que pueda extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos, incluso si estos han sido dispositivos incautados fuera del domicilio del investigado. Por otro lado, la autorización judicial en su caso, debe reunir una serie de requisitos: fija los términos y el alcance del registro, la autorización en su caso para la realización de copias de los datos informáticos, las condiciones necesarias para asegurar la integridad de los datos y la práctica de un dictamen pericial; se insta a realizar copias en lugar de incautar dispositivos; se permite ampliar el registro –en lo que Tejada de la Fuente califica como el aspecto más novedoso de la reforma procesal[895]– cuando existan razones fundadas para considerar que los datos buscados que los datos sean lícitamente accesibles por medio del sistema; y, por último, se recoge que las autoridades y agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria, siempre que de ello no derive

[895] TEJADA DE LA FUENTE, E. ob. cit. p. 187.

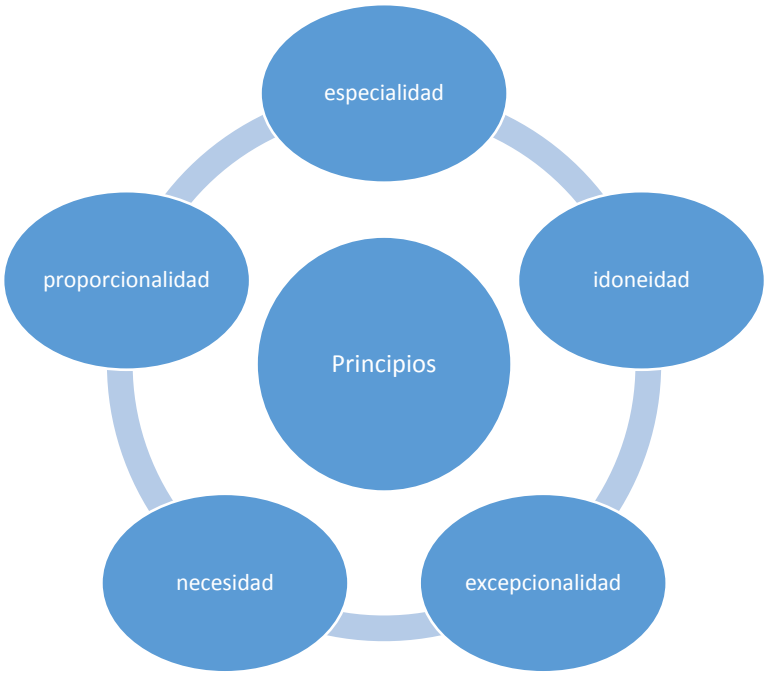
una carga desproporcionada para el afectado, bajo apercibimiento de incurrir en delito de desobediencia.

En lo que concierne al registro remoto, estamos ante una medida que, como subraya Conde-Pumpido, determina un grado tan intenso de injerencia que exige el respeto de límites muy rigurosos, de ámbito material, objetivo y temporal[896]. Este supuesto permite al juez autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos. En todo caso está limitado a un número concreto de delitos particularmente graves; la resolución deberá especificar los dispositivos objeto de la medida, el alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos y el software que se utilizará; los agentes autorizados para la ejecución de la medida; la autorización para la realización y conservación de copias de los datos informáticos; y las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

También merece la pena apuntar la necesaria colaboración por parte de los prestadores del servicio. En este punto, recordar que en las disposiciones referidas a los registros remotos sobre equipos informáticos, se recoge también la necesaria cooperación por parte de los prestadores de servicios. En concreto, el artículo 588 septies b) recoge que están obligados a facilitar a los agentes investigadores la colaboración precisa para la práctica de la medida y el acceso al sistema, y también están obligados a facilitar la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización.

En todo caso para la adopción de cualquiera de las dos medidas, registro de dispositivos de almacenamiento masivo y de registros remotos, es necesaria la autorización judicial y que se respeten los principios señalados en la siguiente figura:

[896] CONDE-POMPIDO TOURÓN, C. La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos (arts 588 sexies y 588 septies LeCrim), *Jornadas de Especialista en Criminalidad Informática*. 10 de marzo de 2016. Disponible en web: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Conde-Pumpido%20Tour%C3%B3n.pdf?idFile=4d9fe168-e9ee-4cd9-a783-68eab6158e47



Fuente: elaboración propia

Son varias por tanto las conclusiones que se pueden extraer de este capítulo. En primer lugar, que sin lugar a dudas la realidad digital produce de nuevo un efecto paradójico en algunas de las realidades preexistentes. Aquí estamos ante una mejora en las posibilidades de investigación por el propio desarrollo tecnológico, con una realidad que es la de la dificultad planteada por motivos de soberanía sobre los que tradicionalmente se ha articulado la jurisdicción entendida en sentido amplio. La naturaleza ubicua y difuminadora de frontera, la balcanización que define la nube, provoca que ámbitos tan tradicionalmente vinculados al principio de la territorialidad, cuales son las actuaciones de las fuerzas de seguridad como los elementos jurisdiccionales, afronten nuevas dificultades.

A ello se suma, como ya hemos visto en otros apartados, de nuevo la necesidad de equilibrio entre, por un lado, defender la legítima capacidad de actuación por parte de las autoridades públicas, y combinarlo con una razonable expectativa de privacidad. Es en realidad una proyección de la clásica dicotomía entre libertad y seguridad que además tiene una repercusión en otros ámbitos como el de la libertad de empresa, por cuanto la afectación que tiene este fenómeno en las posibilidades de negocio de los proveedores es indudable. El

escenario actual, como en tantos otros ámbitos, invita a combinar lo nacional y lo internacional.

Por un lado, cada uno de los Derechos nacionales que ha de estar informado por garantizar la privacidad del usuario y consiguientemente por la necesaria autorización judicial, que habrá de ser previa salvo en supuestos muy tasados y en todo caso marcado por notas de urgencia y de concurrencia de bienes jurídicos superiores.

También en el plano nacional habrá que partir de la posibilidad de que las autoridades requieran a los proveedores radicados en el territorio correspondiente, su correspondiente colaboración. En este sentido son muchos los criterios que se pueden seguir a efectos de considerar esa raíz en el territorio: domicilio social, gestión efectiva, capacidad de control…etc. Cualquiera puede ser válido siempre y cuando sean parámetros objetivos. Se hace igualmente necesario en el marco contractual, que se recoja en todo caso la posibilidad de que el proveedor tenga que dar acceso a los datos de los que es responsable el cliente, sin perjuicio de que dichos requerimientos deberán estar limitados por lo que acabamos de decir y también por la necesaria ubicación de los datos en el territorio correspondiente, sean los originales o una copia de seguridad y acompañado en todo caso de una notificación al cliente, salvo en aquellos casos en los que, de nuevo, nos encontremos, por mor de la autorización judicial ante la concurrencia de un bien jurídico superior, entre los que puede estar incluida, sin duda, la seguridad nacional, concepto en todo caso que exige de una prudente aplicabilidad. La ubicación de los datos es susceptible de ser determinada en tanto en cuanto, como se ha visto en otro apartado, es elemento determinante a la hora de llevar a cabo una transferencia internacional bajo un paraguas o cobertura legal adecuados.

Igual o mayor trascendencia que el plano nacional la tiene el internacional. En aquellos supuestos en que los datos se encuentren radicados en un territorio distinto de aquel sobre el que tiene jurisdicción tanto las fuerzas de seguridad como la autoridad judicial, es necesario recurrir a los mecanismos de cooperación internacional, gocen estos de una mayor realidad integradora, como ocurre en el ámbito de la Unión Europea, o sean los sistemas tradicionales de convenios internacionales o de tratados de asistencia jurídica mutua. La soberanía llega hasta donde llega, y todavía no ha desaparecido.

CONCLUSIONES

PRIMERA:

Existe una nueva generación de derechos que requiere de una atención específica por gozar de una sustantividad propia: los derechos de cuarta generación. Se consideran como tales los derivados del impacto tecnológico y la evolución científica, frente a las anteriores generaciones de derechos que venían informadas por la posición del ciudadano frente al poder político.

Forman parte de dicha categoría, en el ámbito relacionado con la tecnología, dos tipos de derechos: aquellos derechos tradicionales que se han visto cualitativamente afectados por la revolución tecnológica como el derecho a la intimidad y la libertad de expresión; y otros derechos de nuevo cuño, siendo el derecho a la protección de datos el principal exponente del mismo.

En el caso de los derechos tradicionales citados, el impacto de la tecnología ha sido tan considerable que no estamos hablando de una mera adaptación a un nuevo entorno o a una nueva forma de comunicación. Probablemente nunca la intimidad se ha visto tan amenazada; ni la libertad de expresión tan proyectada. Sin embargo, el cambio no es meramente cuantitativo. No es simplemente que hay más amenazas o más posibilidades de expresarse. No, la democratización, universalización y generalización de Internet a partir de mediados de los años noventa han provocado que no se pueda hablar de una vida digital y otra no digital, sino que la vida actual o es digital o no es. Hay un cambio de naturaleza y de entorno en el que no basta una adaptación de los tradicionales y consolidados derechos humanos, ya que se trata de una evolución radical y continua –de ahí lo cualitativo– que interfiere en la concepción tradicional de determinados derechos humanos.

Aun así, el impacto de la tecnología está siendo tan considerable que no basta con la adaptación de derechos y libertades tradicionales, sino que la propia fuerza de las cosas ha provocado el surgimiento de un nuevo derecho fundamental, hoy día poco controvertido en cuanto a su necesidad y reconocimiento: el derecho fundamental a la protección de datos. Se trata de un derecho que ha ido asumiendo nuevos retos conforme se desarrollaban nuevas realidades tecnológicas a las que se ha ido adaptando: desde los teléfonos móviles

hasta la Internet de las cosas, pasando por las redes sociales y, lógicamente, la computación en nube.

SEGUNDA:

Al margen de su virtualidad práctica, es necesario distinguir entre el derecho a la intimidad, el derecho a la protección de datos y el derecho a la privacidad. En el caso de los dos primeros existe ya, a pesar de su interconexión fáctica, un claro reconocimiento doctrinal, normativo y jurisprudencial en cuanto a sus diferencias, principalmente en su ámbito y en su contenido. Por su parte, a nuestro juicio, el derecho a la privacidad en sentido estricto es el derecho que englobaría tanto al derecho a la intimidad –y otros como el derecho al secreto en las comunicaciones, el derecho al honor o el derecho a la propia imagen– en cuanto que derecho de cuarta generación, es decir, en cuanto que derecho afectado por el uso de las nuevas tecnologías, como el derecho a la protección de datos personales. Todo ello sin perjuicio de que en determinadas ocasiones estos dos últimos tengan una interconexión instrumental, en el sentido de que en algunos casos la quiebra del derecho fundamental a la protección de datos puede dar lugar a la vulneración del derecho a la intimidad. Existe una vertiente garantista del derecho fundamental a la protección de datos que se manifiesta también en el entorno *cloud*. La afectación del derecho a la intimidad como derecho de cuarta generación se puede dar por vías distintas de la protección de datos propiamente dicha y consiguientemente goza, reiteramos, de una sustantividad propia. Es decir, podemos tener una intimidad vulnerada por una quiebra del derecho a la protección de datos, podemos tener una quiebra de la protección de datos sin que se vea vulnerado el derecho a la intimidad y podemos tener un derecho a la intimidad vulnerado por la tecnología sin que sea consecuencia de una vulneración del derecho a la protección de datos, al menos con dimensión constitucional. Todo ello a pesar de la *vis atractiva* que ejerce el derecho fundamental a la protección de datos, en muchas ocasiones de manera equivocada.

TERCERA:

El derecho a la intimidad se ha situado en primera línea en cuanto al impacto que ha supuesto en su configuración el desarrollo tecnológico. Existen dos ámbitos en los que queda muy

bien reflejado dicho impacto: el relativo a las investigaciones criminales y policiales y el ámbito de las relaciones laborales.

En el primero de ellos es cada vez más frecuente el necesario examen de si se ha visto afectado el derecho a la intimidad al acceder a la información en dispositivos electrónicos, en particular a los efectos de la obtención de pruebas. Sin perjuicio de que la jurisprudencia siga aplicando la misma filosofía examinadora con la concurrencia de principios habilitantes y los juicios de proporcionalidad, el hecho de que un dispositivo electrónico pueda albergar una ingente cantidad de información y la extraordinaria capacidad de análisis de la misma, suponen un salto exponencial en la tradicional configuración de este derecho. La capacidad de almacenamiento es uno de los servicios más habituales prestados por la computación en nube.

La existencia de toda una nueva problemática cualitativa y no meramente cuantitativa es una realidad que exige la búsqueda, de nuevo, de un adecuado equilibrio entre las necesarias garantías de la persona investigada y las exigencias de investigación acordes con una sociedad tecnológicamente avanzada. Cualquier desequilibrio en uno u otro lado de la balanza supondrían la merma de la libertad o de la seguridad respectivamente. Autorización judicial, legalidad y salvaguarda urgente de un interés superior son algunos de los elementos propios de este equilibrio.

Un impacto comparable ha tenido la tecnología en el derecho a la intimidad del trabajador en el ámbito de la relación laboral. Más allá de otras dimensiones como el teletrabajo o el sindicalismo en línea, en gran medida esa afectación ha venido dada como consecuencia de cómo se han difuminado las fronteras entre la vida personal y profesional por el uso por el trabajador de los dispositivos tecnológicos puestos a su disposición por el empleador. De nuevo se hace necesario un adecuado reequilibrio entre el legítimo poder de dirección del empresario, reforzado por la puesta a disposición de herramientas tecnológicas y su capacidad de vigilancia del trabajador, y la legítima expectativa de respeto a su derecho a la intimidad que este tiene para que no se trascienda el ámbito propio de la actividad laboral.

En cuanto a la articulación normativa, la línea doctrinal de que en la unidad organizativa laboral que corresponda se articulen códigos de conducta respecto al uso de la tecnología se presenta como una herramienta adecuada por cuanto permite combinar la seguridad jurídica, que ambas partes exigen, con la flexibilidad propia de la continua evolución tecnológica y de la progresiva adaptación a los criterios que vayan marcando los tribunales

en la abundante casuística. Este sistema de aproximación normativa resulta adecuado en muchos ámbitos del Derecho de Internet y particularmente para hacer frente a algunos de los retos jurídicos que afronta la protección de datos en la computación en nube.

En cuanto al contenido de los códigos de conducta, es necesario que figuren claramente los supuestos en los que se limita el derecho a la intimidad del trabajador y que, cuando ello suceda, venga acompañado de las oportunas garantías, consustanciales a la quiebra del contenido de cualquier derecho fundamental y máxime en una situación de natural asimetría. Además sería conveniente ir abandonando progresivamente cláusulas abiertas como las de los "usos sociales", que resultan demasiado vagas y cuya concreción en lo tecnológico tiene particulares dificultades.

CUARTA:

El derecho a la libertad de expresión se ha visto exponencialmente acrecentado por el surgimiento de Internet, siendo la viralidad o la obsolescencia del secuestro de publicaciones, realidades que ayudan a comprender el salto cualitativo. La ausencia o reducción a lo insignificante de los conceptos de espacio y tiempo –la natural ubicuidad en el caso de la computación en nube– en internet, hacen que sea difícil aplicar los mecanismos jurídicos tradicionales a la libertad de expresión e información en Internet.

Presupuesto de la libertad de expresión es el principio de neutralidad, que es consustancial a la existencia de la Red de redes tal y como hoy la concebimos, así como el derecho de acceso a la Red, sin el cual la libertad de expresión quedaría vacía de contenido.

Precisamente en relación con esto último cabe subrayar que el derecho de acceso a Internet constituye un presupuesto, en su vertiente jurídica y lógicamente en la tecnológica, para poder hacer realidad el derecho a la libertad de expresión en sí misma, además de muchos otros derechos. En cuanto a su consideración como derecho fundamental en sí mismo y pensando en la trascendencia que esta catalogación puede tener en el plano práctico, su inclusión en el contenido propio del derecho a la libertad de expresión en Internet facilita hoy día su universalización, por cuanto este es un derecho genéricamente conocido, sin perjuicio de que a nuestro juicio tiene que darse una progresiva incorporación normativa en los casos que se pueda, y jurisprudencial cuando la rigidez constitucional lo impida.

QUINTA:

Existen ámbitos muy concretos en los que los límites a la libertad de expresión exigen de una particular actuación por parte de los poderes públicos y una inevitable colaboración por parte de los actores privados. Sirvan como ejemplo la protección de la juventud y de la infancia o los límites a los discursos de odio. En determinados casos, el daño que la superación de los límites de la libertad de expresión puede causar en Internet exige incluso que los límites vayan más allá de los establecidos para el mundo *off line*. No se está defendiendo un excepcionalismo, sino que se propugna que, dentro de la tradicional técnica de ponderación de derechos fundamentales, el fenómeno de la viralidad sea introducido en la ecuación. Por lo tanto, misma técnica de ponderación en el caso concreto y de aplicación de la misma filosofía de examen, pero que no tiene por qué, precisamente por el vector tecnológico, derivar en idénticas conclusiones.

SEXTA:

Protagonistas indiscutibles en el ejercicio de la libertad de expresión en Internet son los intermediarios, que son los que hacen factible no solo la nueva dimensión cuantitativa de los derechos antes mencionados, y en particular de la libertad de expresión, sino también, y esto es lo relevante, su componente cualitativo.

La evolución jurisprudencial ha ido desarrollando las pautas fijadas por la normativa europea en cuanto al régimen de responsabilidad de los intermediarios en internet. Sigue constituyendo uno de los elementos de mayor controversia, aunque existe una tendencia hacia unas líneas relativamente claras de actuación. Se trata de un régimen jurídico de gran impacto en cuanto a los límites a la libertad de expresión en internet. El elemento colaborativo de la información en la web, la democratización de la creación y de la recepción de contenidos y la estructura extremo a extremo que está en la misma esencia de la Red, tal y como hoy la conocemos, hacen que equilibrio, prudencia y actuación solamente en los casos más graves, sean la aproximación razonable. Sin alterar la filosofía que hoy subyace en el régimen de responsabilidad, la adopción progresiva de mecanismos de autorregulación por parte de los prestadores que gocen del reconocimiento de las autoridades públicas y que vayan incorporando las tendencias jurisprudenciales parece una línea de trabajo adecuada.

Idéntica reflexión en cuanto a grandes principios, colaboración de la industria y progresiva incorporación de la realidad social a través de la jurisprudencia, es aplicable a algunas de las problemáticas más desafiantes de la computación en nube.

SÉPTIMA:

El derecho fundamental a la protección de datos personales constituye uno de los derechos de cuarta generación por excelencia. Sin perjuicio de antecedentes oficiales en los años sesenta, surge normativamente en los setenta, llegándose a la constitucionalización en algunos supuestos, se desarrolla internacionalmente a principios de los ochenta y tiene su despliegue legislativo en los noventa.

La regulación de este derecho ha de ser principialista. Esta forma de ordenación jurídica debe impregnar de manera inevitable cualquier acercamiento normativo a los impactos de la tecnología en la vida social. Sin entrar en mayores disquisiciones, la velocidad a la que evoluciona la tecnología hace que sea imprescindible una cierta inteligencia normativa y dejar el detalle a los supuestos que sean absolutamente inevitables. Además, la construcción principialista favorece los necesarios pactos internacionales. El principio de calidad de los datos, y todas las consecuencias que de él se derivan, debe seguir constituyendo el eje sobre el que gire cualquier regulación. Es el sujeto el titular de los datos el que en principio debiera decidir qué, cuándo, dónde, quién y por cuánto tiempo se han de tratar sus datos, sin perjuicio de las lógicas matizaciones y cautelas que exige la propia convivencia social y los presupuestos extraordinarios que bajo las oportunas garantías justifiquen actuaciones por parte de otros sujetos.

Los citados detalles han de ser lógicamente canalizados por los sujetos normativos tradicionales pero viéndose complementados por una triple vía: el más que demostrado papel que juegan las autoridades judiciales en la adaptabilidad del Derecho de Internet, la inevitable colaboración de la industria y del resto de actores del entorno tecnológico a través de mecanismos de autorregulación oportunamente validados y el creciente papel de las autoridades de protección de datos. Estos órganos son sujetos necesarios, sin duda, y deben, a través de una adecuada coordinación internacional, garantizar la seguridad jurídica que la vida social en general y el tráfico económico en particular exigen y la flexibilidad impuesta por la realidad evolutiva que la tecnología nos demuestra a diario.

OCTAVA:

En el plano tecnológico la nube, como recurso centralizado para la prestación integral de servicios a través de la Red sobre la base de la necesidad y la demanda de los clientes, supone dar a los consumidores, negocios, gobiernos y cualquier usuario, la posibilidad de acceder a enormes recursos informáticos desde cualquier dispositivo y en cualquier lugar en que haya acceso a la red. Con independencia de que se trate de un fenómeno evolutivo, de que se haya dado una convergencia de realidades tecnológicas ya existentes, de que se haya cerrado un círculo histórico, lo cierto es que estamos ante una tecnología que se ha ganado su sustantividad propia por la fuerza de los hechos. No se conoce una tecnología que no traiga causa de otra preexistente. La tecnología es evolutiva, aunque se califique de disruptiva, este sí es un concepto más "marketiniano" que tecnológico. La grandeza de esta evolución tecnológica es que viene derivada de la convivencia y del intercambio. Basta recordar los famosos *Request for Comments* de la comunidad científica y académica. Aunque sea circular en el plano conceptual (de compartir a individualizar y vuelta a compartir), no pierde su dimensión evolutiva. Es puro darwinismo tecnológico: son las tecnologías que sobreviven las que sirven al desarrollo de otras. A ello se añade su dimensión finalista, ya que el cloud ha conseguido acercar los recursos a cualquier consumidor sin importar el dispositivo con el que se acceda. Ha facilitado la vida al usuario. Si a ello le añadimos su dimensión de negocio, insistimos que sí se ha hecho merecedor de un reconocimiento individualizado sin el cual perdería cierto sentido este trabajo.

NOVENA:

Desde el punto de vista económico, la computación en nube se encuentra particularmente ligada a la perspectiva de negocio y está llamada a ofrecer resultados en los planos microeconómico y macroeconómico, ambos elementos a tener en cuenta a la hora de ponderar los retos asumidos por la protección de datos. Particular importancia tiene la vertiente microeconómica, que viene informada por la reducción de las barreras de entrada, la escalabilidad, la ubicuidad, la adaptabilidad, el pago por uso y la garantía ante el desastre, lo que hace esta tecnología particularmente atractiva para las PYMES.

DÉCIMA:

La cuasi universalización de la aplicabilidad del RGPD tiene consecuencias directas en la computación en nube. En concreto un proveedor de servicios en nube se verá sometido a la normativa europea cuando actúe como encargado y se encuentre radicado en la Unión Europea, esté o no el responsable en la UE; cuando actúe como encargado y esté fuera de la UE, pero el responsable esté en la UE o estando fuera de la UE ofrezca bienes y servicios o monitoree a interesados en la UE; o bien cuando directamente ofrezca como responsable bienes y servicios o monitoree a interesados en la UE o en el marco de las actividades de un establecimiento en la UE.

En cuanto a conceptos conexos y relevantes por su inclusión en la normativa europea, consideramos que el concepto de "establecimiento" no es aplicable a las herramientas o instrumentos de carácter técnico y por tanto tampoco a un centro de datos o a una granja de servidores, que serían un equipamiento técnico. En relación con el concepto "contexto de las actividades" se ha consolidado progresivamente una interpretación extensiva, incluyendo las actividades indisociablemente ligadas aunque la entidad en territorio europeo desempeñe o no un papel concreto en el tratamiento de los datos e incluyéndose cualquier centro organizativo de naturaleza comercial, publicitaria o de gestión de negocio que tenga una misión hacia terceros que vaya más allá del componente técnico.

UNDÉCIMA:

A pesar de la frecuente asimetría de las partes en la contratación de servicios en nube, con base en la vigente normativa sobre protección de datos, la posición del proveedor de este tipo de servicios es genéricamente la de un encargado del tratamiento, correspondiendo al cliente la determinación de los fines y de los medios del mismo y por tanto la posición de responsable. Esta situación únicamente quebrará y dará lugar a la corresponsabilidad, cuando trate datos para sus propios fines, cuando ofrezca sus servicios al usuario final en el marco de relaciones B2C o bien cuando lleve a cabo cualquier determinación respecto de aspectos esenciales del tratamiento de datos, es decir, cuando su aportación en cuanto a los medios vaya más allá de la lógica discrecionalidad técnica.

Al margen de la previsión normativa, el desequilibrio entre las partes que resulta tan habitual en la computación en nube exige que cuando se trate de contratos de adhesión se articulen

mecanismos que salvaguarden la distribución tradicional de responsabilidades. En este sentido, más allá del necesario impulso de los códigos de conducta, los mecanismos de certificación y las cláusulas modelo que impulsa el RGPD, la articulación de un sistema de registro de condiciones contractuales para la nube avalado o certificado por la autoridad de control de cada país resultaría igualmente de utilidad. Esta suerte de mecanismo de transparencia y de garantía contribuiría también a la seguridad en el tráfico jurídico y a la salvaguarda del derecho fundamental a la protección de datos.

En conclusión, el régimen actualmente vigente que favorece los mecanismos de autorregulación supervisados por la autoridad pública –códigos o certificaciones– o las condiciones contractuales estandarizadas, es positivo para la computación en nube, sin perjuicio de que se articule algún mecanismo añadido que refuerce dicha supervisión y que flexibilice para la computación en nube las rigideces a las que el modelo de clausulado único podría llevar.

DUODÉCIMA:

El contrato de servicios en nube es habitualmente un contrato de adhesión que consta por escrito, de naturaleza mercantil en el esquema B2B, informático y que tiene como objeto la prestación de servicios tecnológicos y más concretamente la puesta a disposición de unos medios o recursos tecnológicos conforme a unas exigencias establecidas en el Acuerdo de Nivel de Servicio (SLA).

El contrato de servicios en nube presenta un doble contenido que a su vez habitualmente se proyecta en su estructura: el contrato marco, que recoge los elementos consustanciales a cualquier modalidad contractual, y el ya citado Acuerdo de Nivel de Servicio, que contempla normalmente los aspectos técnicos del servicio prestado. Este último debe incluir los objetos de nivel de servicio en cuanto a la ejecución técnica, a la seguridad, a la gestión de los datos y a la protección de estos.

En referencia a la protección de los datos, el RGPD es una norma más exigente o al menos más detallista en cuanto al contenido, algo que resulta lógico por la utilización del instrumento jurídico del reglamento comunitario. Resulta particularmente conveniente para el tráfico económico y la seguridad jurídica, una vez más, la articulación de vías sustitutivas que gocen

de la misma validez, como la adhesión a un código de conducta, el sometimiento a un mecanismo de certificación o la utilización de modelos de cláusulas contractuales.

En definitiva el contrato entre el prestador de servicios cloud y el cliente será un contrato de prestación de servicios que deberá hacerse constar por escrito; que responderá habitualmente a un esquema de adhesión; con una estructura dual de contrato marco y anexos, siendo dentro de estos el SLA y, en su caso, el PLA, los más relevantes. En el apartado o cláusula específica de la protección de datos, se deberá incluir un contenido mínimo recogido en el RGPD, sin perjuicio de su eventual sustitución parcial, en el plano de las garantías, por las fórmulas de adhesión a mecanismos de estandarización específicos para la computación en nube.

El contrato debe verse además no solo como el tradicional instrumento generador de obligaciones entre las partes, sino que juega un papel clave como como elemento de *compliance*, de garantía para el cliente/responsable y frente a terceros, tanto autoridades como interesados, máxime considerando el alto grado de detalle que se exige en cuanto a su contenido. En el ámbito cloud, además, resulta particularmente conveniente el recurso a los códigos de conducta. En este punto es digno de destacar, como ya se ha dejado ver a lo largo del texto, el trabajo realizado por la industria en el grupo constituido por los proveedores y amparado por la Comisión Europea. Si este código culmina, puede, sin duda, convertirse en un estándar normalizado, bajo el paraguas del art. 40 RGPD, que dote de seguridad jurídica al proveedor, de garantías al cliente y de protección a los interesados que ponen sus datos en manos de los anteriores. La promoción de estos sistemas constituye una obligación, ex. art. 40.1 RGPD, de los Estados miembros, las autoridades de control, el Comité y la Comisión. La asimetría del cloud, incluso en el entorno B2B que nos ocupa, lo destaca como un elemento llamado a jugar un papel creciente.

Idénticas reflexiones cabría realizar respecto de los modelos de cláusulas, que tan importante papel han jugado, por ejemplo, en las transferencias internacionales. Lo cierto es que a nuestro juicio no es tanta la diferencia en el plano material entre un código de conducta o el modelo de cláusulas. Ambos instrumentos servirán, no solo a los efectos de demostrar algunas exigencias normativas del RGPD, sino que contribuirán a la seguridad jurídica y a la competitividad económica. Su procedimiento, más sencillo que el normativo, les lleva a desempeñar un papel clave en el mundo jurídico-tecnológico y el cloud no es sino un ejemplo.

DECIMOTERCERA:

Los derechos que corresponden a los interesados siguen siendo una de las proyecciones del contenido esencial del derecho a la protección de datos y se han visto aumentados en el RGPD. De los nuevos derechos que se recogen (derecho al olvido, a la limitación del tratamiento, a la portabilidad y a la oposición a las decisiones individuales automatizadas), a nuestro juicio, únicamente goza de sustantividad propia el derecho a la portabilidad, pudiéndose haber incardinado los otros en los derechos de supresión o de oposición.

En cuanto al derecho a la información, jurisprudencia y autoridades de protección de datos lo vienen reconociendo como un auténtico derecho, pero a nuestro juicio –y siendo consciente de la teoría de las situaciones jurídicas subjetivas– se trata de una obligación, ya que es algo que recae sobre el responsable sin necesidad de requerimiento alguno por parte de los interesados, a diferencia de lo acaecido con el resto de derechos.

El denominado *data intervenability*, que se define precisamente como la capacidad del proveedor de asistir al cliente a la hora de facilitar el ejercicio de los derechos de los interesados adquiere una particular relevancia en el entorno de la nube, fundamentalmente debido a las notas de asimetría, deslocalización, estructura distribuida y cadenas de subcontrataciones. Se hace en este sentido lógica, más que en otras tecnologías, la tendencia a que la asistencia y cooperación del proveedor que exige el RGPD se concrete en una satisfacción directa de todos los derechos en nombre del responsable en aquellos casos en que sea posible, siendo necesario que se recoja claramente en el contrato suscrito entre las partes o bien en cualquiera de los instrumentos válidos ya mencionados (códigos, mecanismos de certificación y modelos de clausulado). Esa concreción se deberá recoger a través de los oportunos protocolos en el Acuerdo de Nivel de Servicio y es adecuado que su verificación se canalice a través de uno de los citados instrumentos o de la correspondiente auditoría.

DECIMOCUARTA:

Interoperabilidad, estandarización y neutralidad, conceptos todos ellos diferentes, son presupuestos necesarios para una adecuada satisfacción del derecho de portabilidad.

Con independencia del reconocimiento del derecho a la portabilidad como mandato jurídico en el RGPD, la realidad es que la portabilidad ya era posible hoy día por vía jurídica y por

vía tecnológica, contemplándose en el contrato en la primera y a pesar de las potenciales dificultades y costes en la segunda, y constituyendo simplemente un elemento comercial dentro de la necesaria y lógica competitividad tecnológica.

En el RGPD no estamos hablando de un derecho susceptible de ser aplicado en el marco de las relaciones B2B, sino que se trata de un derecho que le corresponde al interesado titular de los datos respecto del responsable de los mismos. Cuestión distinta es que, al igual que con el resto de derechos, sea inevitable que el proveedor cumpla con los mismos parámetros que los establecidos para el responsable con la finalidad de que la portabilidad de los datos en ese entorno de nube en el que se está dando el tratamiento por cuenta de terceros sea realmente efectiva. No obstante estamos en la vertiente de la libertad contractual que es inspiradora, más allá de las lógicas previsiones normativas, de las relaciones B2B y que además viene siendo incorporada a los códigos de conducta en los que ya se está trabajando.

A mayor abundamiento, lo que se ha planteado como una novedad en el RGPD en el plano de los derechos del interesado, ya existe en cierta medida en ordenamientos como el español, a través de las indicaciones de la Agencia, en el marco de las relaciones B2B, por cuanto se contempla el régimen de reversibilidad (devolución *in house*) pero también se recoge la posibilidad de devolución al encargado designado por el responsable, lo que supone una portabilidad entre encargados en sentido estricto.

En cuanto a las vertientes de las cláusulas de salida, una vez más las certificaciones juegan un papel clave, máxime en una tecnología que está basada en un sistema de multiposesión, en un continuo dinamismo y en una cadena de subcontrataciones. Será esta la vía más adecuada para garantizar al responsable, en primer lugar, y a los interesados en último, que los datos no permanecen en manos del proveedor, más allá de lo que venga exigido por disposiciones normativas que, en todo caso, deberán estar limitadas, en pro del principio general de calidad de los datos, al tiempo estrictamente necesario para el cumplimiento de las mismas.

En conclusión, el esquema de portabilidad en la nube en el seno de las relaciones B2B es perfectamente factible con base en el actual régimen jurídico e incluso parcialmente obligatorio en algún ordenamiento, formando parte de la libertad contractual y constituyendo un elemento de sana competitividad económica.

DECIMOQUINTA:

El fenómeno de las transferencias internacionales, en lógica con la característica del acceso ubicuo, es bastante frecuente en la computación en nube. El RGPD articula un sistema de transferencias internacionales muy similar al existente previamente, basado en el concepto de nivel equivalente de protección, aunque con alguna modulación que puede resultar de particular interés para la computación en nube. En el caso de las transferencias internacionales basadas en una decisión de adecuación, se recoge la posibilidad de que sea, no solamente a un país, sino también a uno o varios sectores específicos de un país. Los proveedores de servicios en nube encajan a la perfección dentro del concepto de sector específico, si bien es cierto que su virtualidad para la nube podría perder efectividad al estar circunscrito al sector en un tercer país y sobre todo, porque a la hora de adoptar la decisión, los parámetros a tener en cuenta no se entenderían sin dicho elemento territorial.

Sin lugar a dudas, como en tantos otros aspectos, la articulación de un modelo de clausulado que permita la posibilidad de realizar transferencias internacionales de datos con las oportunas adaptaciones a los aspectos esenciales de la nube, como por ejemplo en cuanto a las formalidades contractuales o los sistemas de auditoría, sería una práctica que dotaría de seguridad jurídica al tráfico y daría garantías, particularmente en el caso de las PYMES. El RGPD no impide en ningún momento la posibilidad de que exista un modelo de clausulado general y otro específico de la computación en nube, tal y como ya hemos apuntado y recomendado en conclusiones anteriores.

Idénticos efectos favorables pueden tener los códigos de conducta y los mecanismos de certificación, aunque la redacción del RGPD a nuestro juicio desvirtúa ambos mecanismos y nos lleva a una mezcolanza de todos ellos. Por un lado, los códigos o certificaciones en sí mismas han de ser autorizados ex art. 40 RGPD por una autoridad de control o por la Comisión. Ello en principio parece lógico. Sin embargo, la adhesión por parte del proveedor a un código o a un mecanismo de certificación, aprobado por las referidas autoridades y que ofrece suficientes garantías, parece no compadecerse con la necesidad añadida en el caso de las transferencias internacionales de asumir compromisos jurídicamente vinculantes y exigibles. De hecho, una previsión de este tipo empequeñece la utilidad de estos instrumentos y debería eliminarse.

DECIMOSEXTA:

Si las transferencias internacionales son muy frecuentes en la computación en nube, se puede afirmar que la subcontratación es consustancial a la nube, fundamentalmente porque es la que permite en gran medida cumplir con dos de sus notas más características: la escalabilidad y la elasticidad, significando la primera que los recursos pueden ampliarse o contraerse en función de las necesidades del cliente y la segunda que esa expansión o contracción se puede hacer rápidamente.

Con la finalidad de garantizar la transparencia es necesario que el cliente tenga la posibilidad de conocer a quién y qué se subcontrata en todo momento. En este sentido resulta equilibrado, como han hecho las agencias española o alemana, un "encadenamiento de información" revestido jurídicamente y dotado de flexibilidad. Esto implica un contrato lógicamente suscrito entre el proveedor y sus subcontratistas y que exista una web dinámica para que el cliente pueda acceder a la información –y en su caso oponerse a la subcontratación– en todo momento. Este sistema de actualización a través de la web reúne la doble condición de otorgar la seguridad jurídica que el cliente quiere, y permitir la flexibilidad necesaria que el servicio exige. Con este criterio estamos asistiendo a una modulación razonable de lo previsto en el artículo 21 ROPD y satisfaciendo el fundamento último de las previsiones normativas allí establecidas, cierto es que con un nivel de diligencia "in vigilando". En definitiva, aceptando una ligera modulación a través de los pronunciamientos de las autoridades de supervisión, estamos simplificando el régimen jurídico, sin mermar la seguridad jurídica, y permitiendo el crecimiento económico vinculado al entorno de la nube.

En este campo de las transferencias y de la subcontratación, las BCR pueden jugar un papel clave si se desvinculan del grupo multinacional y se convierte en el paraguas jurídico del proveedor/encargado y sus correspondientes subcontratistas. A nuestro juicio la redacción del actual RGPD ayuda, y mucho, a esta posibilidad. Hasta ahora las BCR para los encargados de tratamiento únicamente se pueden realizar en el seno de un mismo Grupo multinacional. Sin embargo, la nueva regulación de las BCR puede dar entrada a esta posibilidad ya que se podría dar cabida a la prestación del servicio bajo el paraguas de "la unión de empresas dedicadas a una actividad económica conjunta" a la que hace referencia el art. 47.1 RGPD. Es decir, a día de hoy, existe la posibilidad de que las BCR sean utilizadas intragrupo, cuando el encargado y el subencargado pertenezcan al mismo Grupo. El RGPD

creemos que puede estar abriendo la puerta a que se desvinculen del grupo corporativo multinacional y sean una vía más que adecuada para los prestadores de servicios en nube, junto con sus subcontratistas. De nuevo seguridad jurídica, con la supervisión de una autoridad pública, pero acompañada de la flexibilidad consustancial a la nube.

DECIMOSÉPTIMA:

La seguridad constituye, hoy día más si cabe, uno de los elementos fundamentales que informan la normativa de protección de datos. Está en las máximas prioridades de las autoridades oficiales y de la propia industria.

Existen normas o al menos principios que son perfectamente trasladables, a través de los lógicos ajustes, al esquema de la computación en nube. Bien es cierto que se ha perdido una oportunidad para introducir en el RGPD disposiciones específicas referidas a la computación en nube, aunque el propio desarrollo tecnológico y la diferente velocidad con respecto a la normativa hacen que ajustes normativos demasiado detallados estén condenados a la caducidad.

Cualquier sistema que se implante tiene que ir acompañado en la nube por un cierto grado de dinamismo y flexibilidad, o de escalabilidad en la seguridad. El ajuste del nivel de seguridad al nivel de riesgo es el vector que ha de seguir informando tanto la vertiente tecnológica como la proyección jurídica de la seguridad, acompañada igualmente del lógico equilibrio con el estado de la técnica y los costes del sistema. La seguridad absoluta no existe y no se le puede pedir a ningún proveedor, pero la articulación de sistemas que minimicen los riesgos con base en el estado de la técnica, de protocolos de actuación ante posibles vulnerabilidades, de una asunción de responsabilidad en la cadena de subcontrataciones y de una implicación de todos los actores contribuirá a hacer de la computación en nube una tecnología de éxito.

Con base en la tendencial asimetría que existe entre las partes, consideramos que los mecanismos de auditoría y certificación son los más adecuados, siempre que estos se ajusten a los esquemas normativos fijados y con un cierto grado de supervisión por parte de las autoridades de protección de datos, con la finalidad instrumental una vez más de salvaguardar el negocio del proveedor y dotar de una cierta seguridad jurídica al cliente en cuanto que responsable; así como una finalidad última de proteger el derecho fundamental

de los interesados. Tanto auditorías –ciertamente por parte de terceros– como certificaciones son mecanismos recogidos en el actual régimen jurídico y consiguientemente aplicables, e incluso recomendables, para el fenómeno del *cloud computing*.

DECIMOCTAVA:

En lo que concierne al acceso a la información en la nube por parte de las autoridades públicas, es necesario el equilibrio entre, por un lado, defender la legítima capacidad de actuación por parte de las autoridades públicas y, por otro, combinarlo con una razonable expectativa de privacidad. Es en realidad una proyección de la clásica dicotomía entre libertad y seguridad que además tiene una repercusión en otros ámbitos como el de la libertad de empresa, por cuanto la afectación que tiene este fenómeno en las posibilidades de negocio de los proveedores es indudable.

La realidad digital produce de nuevo un efecto paradójico en algunas de las realidades preexistentes. Aquí estamos ante una mejora en las posibilidades de investigación por el propio desarrollo tecnológico, con una realidad que es la de la dificultad planteada por motivos de soberanía sobre los que tradicionalmente se ha articulado la jurisdicción entendida en sentido amplio. La naturaleza ubicua y difuminadora de fronteras que define la nube, provoca que ámbitos tan tradicionalmente vinculados al principio de la territorialidad, cuales son las actuaciones de las fuerzas de seguridad y los elementos jurisdiccionales, afronten nuevas dificultades. El escenario actual, como en tantos otros ámbitos, invita a combinar lo nacional y lo internacional.

Por un lado, cada uno de los Derechos nacionales ha de estar informado por la necesidad de garantizar la privacidad del usuario y consiguientemente por la necesaria autorización judicial, que habrá de ser previa salvo en supuestos muy tasados, y en todo caso informado por notas de urgencia y de concurrencia de bienes jurídicos superiores. También en el plano nacional habrá que partir de la posibilidad de que las autoridades requieran a los proveedores radicados en el territorio correspondiente su colaboración. En este sentido son muchos los criterios que se pueden seguir a efectos de considerar esa raíz en el territorio: domicilio social, gestión efectiva, capacidad de control…etc. Cualquiera puede ser válido siempre y cuando se trate de parámetros objetivos. Se hace igualmente necesario en el marco contractual que se recoja en todo caso la posibilidad de que el proveedor tenga que dar

acceso a los datos de los que es responsable el cliente, sin perjuicio de que dichos requerimientos deberán estar limitados por lo que acabamos de decir y también por la necesaria ubicación de los datos en el territorio correspondiente, sean los originales o una copia de seguridad, y acompañado en todo caso de una notificación al cliente, salvo en aquellos casos en los que, de nuevo, nos encontremos, por mor de la autorización judicial, ante la concurrencia de un bien jurídico superior, entre los que puede estar incluida, sin duda, la seguridad nacional, concepto en todo caso que exige de una aplicación prudente.

Igual o mayor trascendencia que el plano nacional la tiene el internacional. En aquellos supuestos en que los datos se encuentren radicados en un territorio distinto de aquel sobre el que tienen competencia tanto las fuerzas de seguridad como la autoridad judicial, será necesario recurrir a los mecanismos de cooperación internacional, gocen estos de una mayor realidad integradora, como ocurre en el ámbito de la Unión Europea, o sean los sistemas tradicionales de convenios internacionales o de tratados de asistencia jurídica mutua, que lógicamente exigen, en virtud de la realidad tecnológica, de una agilización de los procesos.

DECIMONOVENA:

La computación en nube, en cuanto que tecnología con sustantividad propia, plantea determinados retos a la privacidad en general y al derecho a la protección de datos en particular. Bajo esa apariencia que consigue la nube, bajo esa sensación de cercanía al cliente que conlleva la ubicuidad, la nube supone asumir retos de gran calado informados principalmente por la falta de control y de transparencia. Es una suerte de efecto anestesia que tiene el cliente. Una de las grandes ventajas del cliente, el acceso sin necesidad de conocimientos técnicos a alta tecnología y también a importantes mecanismos de seguridad, sin embargo tiene como contrapartida el sometimiento a un tercero que en determinadas ocasiones puede afectar a elementos críticos.

Especial relevancia tienen los retos concernientes a la privacidad. Estamos hablando de aspectos como la responsabilidad que asume cada uno de los sujetos que participa del contrato; de cómo la determinación de la normativa aplicable y la jurisdicción competente vendrán determinados, en parte, por la ubicación geográfica de dichos datos; de cómo el carácter transnacional de la nube, que es nota característica en muchas ocasiones, hace determinante el régimen de las transferencias internacionales de datos; de cómo las cadenas de subcontrataciones no deben debilitar la necesaria robustez de la seguridad; de cómo las

medidas de seguridad aplicables se correspondan con la criticidad de la información; de que se apliquen unos criterios de transparencia que expongan claramente las posibilidades de acceso a la información por parte de las autoridades púbicas.

No obstante, ninguno de dichos retos constituye un elemento determinante para rechazar el potencial económico, medioambiental y social que tiene esta modalidad de servicio computacional para los operadores económicos. A nuestro juicio, la totalidad del ciclo de los datos que son tratados en la nube está protegido. Consideramos que *per se* ninguno de los retos se transforma en riesgo por superar determinados umbrales que deriven en una conculcación de la privacidad del cliente del proveedor o de los clientes de aquel.

Asimismo opinamos que no es necesaria una normativa específica de privacidad para este tipo de tecnología, sino que basta con aplicar las normas actualmente vigentes para que los riesgos se minimicen hasta un nivel asumible en el tráfico jurídico. Sí que es necesaria la oportuna modulación en algunas ocasiones, que venga marcada por una leal colaboración en el plano internacional, una construcción normativa primaria de tendencia principialista, una adecuada supervisión por parte de las autoridades públicas, y mecanismos de autorregulación por parte de la industria.

Este sistema normativo, perfectamente encajable en el régimen jurídico actual (e incluso potenciado en el RGPD a través de los códigos de conducta, los mecanismos de certificación y los diferentes modelos de clausulado, incluso específicos para la nube), permite satisfacer la flexibilidad que exige este tipo de computación, combinándola –en un sano equilibrio– con la seguridad jurídica que demandan los clientes de la misma y, en último lugar, con la salvaguarda del derecho a la protección de datos de los ciudadanos.

BILIOGRAFÍA

ARTÍCULOS Y MONOGRAFÍAS

- AA.VV. *The Federalist. A Commentary on the Constitution of the United States; Being a Collection of Essays Written in Support of the Constitution Agreed Upon September 17, 1787, by the Federal Convention*. Editado por LODGE H.C, Nueva York, Putman's, 1889, 586 p. Disponible en web: www.forgottenbooks.com, 2008.
- ABBATE, J., *Inventing the Internet.* Cambridge, Massachusetts, MIT Press, 1999, 264 p.
- ALEXY, R., Hauptelemente meiner Philosophie des Rechts. Traducción de OLIVER LALANA, A.D, DOXA, *Cuadernos de Filosofía del Derecho*, 2009, núm. 32, p. 67-84.
- ALGAN, B., Rethinking "Third Generation" Human Rights, *Ankara Law Review*, Summer, 2004, vol 1, nº 1, p. 121-155.
- ALJAHDALI, H., ALBATI, A., GARRAGHAN, P., TOWNEND, P., LAU, L., y XU, J. Multi-tenancy in Cloud Computing. *8th IEEE International Symposium on Service Oriented System Engineering. SOSE 2014.* Oxford. United Kingdom, April 7-11, 2014. IEEE Computer Society 2014. p. 344-351.
- ALVAREZ CARO, M. Análisis de la sentencia de invalidez del acuerdo de puerto seguro (*safe harbour*). *Revista de Privacidad y Derecho Digital*. abril 2016. nº 3. p.73-110.
- ANDERSON, C. The Web Is Dead. Long Live the Internet. *Wired.* Agosto de 2010.
- ANDREWS, D.C. y NEWMAN, J.M. Personal Jurisdiction and Choice of Law in the Cloud. *Maryland Law Review.* 2013, vol. 73, Issue 1, p. 313-384.
- ANTIC, M., LAGEMAAT, A., VAN DER SLOOT, B., y VAN STEKELENBURG, M., Dutch National Report, *International League of Competition Law (LIDC),* Congress, Oxford, 22-24/September/2012.
- ARAIZA, A.G., Electronic Discovery in the Cloud. *Duke Law and Technology Review*. 2011. nº 10. p. 1-19.
- AREITIO, J. Protección del *Cloud computing* en seguridad y privacidad. *REE.* mayo de 2010.
- ARMBRUST, M., FOX, A., GRIFFITH, R., JOSEPH, A.D., KATZ, R.H., KONWINSKY, A., LEE, G.L, PATTERSON, D.A., RABKIN, A., STOICA, I. y ZAHARIA, M. Above the Clouds: A Berkeley View of Cloud computing. *Magazine Communications of the ACM*. April 2010, vol. 53, issue 4, p. 50-58.
- ASPAS, J.M., Derechos humanos y nuevas tecnologías: el derecho a la autodeterminación informativa; en CONTRERAS. M., POMED. L, y SALANOVA. R. (coord.), *Nuevos escenarios y nuevos colectivos de los derechos humanos. Conmemoración del cincuenta aniversario de la Declaración Universal de Derechos Humanos*, Monografías de la Revista Aragonesa de Administración Pública, 1998, p. 357-399.
- BALLUGUERA GÓMEZ, C. Diferencias entre el contrato por adhesión y el contrato por negociación. www.notariosyregistradores.org. Disponible en web:

http://www.notariosyregistradores.com/CONSUMO/ARTICULOS/2014-diferencias-contratos-adhesion-negociacion.htm

- BALKIN, J.M., Digital speech and democratic culture. *New York University Law Review*, 2004, vol. 79, nº 1, p. 1-55.
- BANKS, T., Supreme Court of Canada to Police: Get a Warrant to Search Computers and Mobile Phones [en línea], *Privacy and Cybersecurity Law*, 8 de noviembre de 2013. Disponible en web: http://www.privacyandcybersecuritylaw.com/supreme-court-of-canada-to-police-geWall t-a-warrant-to-search-computers-and-mobile-phones
- BARCELÓ, R. Cloud Computing: Privacy Risks and EU Policy Considerations*. The Future of Cloud Computing* 26 de enero de 2010.
- BARTOLI, E. Data transfers in the cloud. *Expert Group on Cloud Computing Contracts. European Commission*. 28 de marzo de 2014.
- BAYRAK, E., CONLEY, J.P., WILKIE, S. The Economics of Cloud Computing. *The Korean Economic Review*. September 2009. Vol., nº 27, p. 203-220.
- BEHAR QUIÑONES, G. y YAÑEZ FIGUEROA, A. *Introducción a los contratos tecnológicos*. Guadalajara, México. ITESO. 2014. 157 p.
- BELTRÁN PARDO, M y SEVILLANO JAÉN, F. *Cloud Computing, tecnología y negocio*. Editorial Paraninfo. 2013. 167 p.
- BERNERS-LEE, T., Long Live the Web: A Call for Continued Open Standards and Neutrality, *Scientific American,* 22 de noviembre de 2010
- BRAVIN, J., Supreme Court: Police Need Warrants to Search Cellphone Data, *Wall Street Journal*, 25 de junio de 2014. Disponible en Web: http://www.wsj.com/articles/high-court-police-usually-need-warrants-for-cell-phone-data-1403706571
- BURNETT, R. Cloud computing and data protection. *Icaew.* p. 13-15.
- BUSTAMANTE DONÁS, J., Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica, *Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Información*, septiembre 2001, nº 1, p. 3.
- BUYYA, R., BROBERG, J. y GOSCINSKY, A.M. *Cloud Computing: Principles and Paradigms*. Willey. 2011. 664 p.
- CABARCAS ÁLVAREZ, A., PUELLO MARRUGO, P. y CANABAL MESTRY, R. Cloud Computing: tecnología verde como estrategia para la responsabilidad social empresarial. *Saber, Ciencia y Libertad*. 2012, vol. 7, nº 2, p. 135-142.
- CABEZUDO RODRÍGUEZ, N. Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal. en AA.VV. *I Jornada del Boletín del Ministerio de Justicia: «Las reformas del proceso penal»*. Febrero de 2016 Año LXX. Núm. 2186.
- CANALES GIL, A. El derecho fundamental a la protección de datos de carácter personal. *Revista Jurídica de Castilla y León.* abril 2007, nº 12, p. 13-56.
- CARDONA RUBERT, M.B., Las relaciones laborales y el uso de las tecnologías informáticas [en línea], *Lan harremanak: Revista de relaciones laborales*, 2003, nº Extra 1, p. 157-173.

- CARR, N. *The Big Switch: Rewiring the World, from Edison to Google.* W. W. Norton. 2008. 224 p.
- CASCIOTTI VIGNOLO, S. y NAHABETIÁN BRUNET, L. Cloud Computing & Walled Gardens. *Revista de Derecho de la Universidad de Montevideo*. 2012. nº 21. p 23 y siguientes.
- CASTELLS, M., Internet, libertad y sociedad: una perspectiva analítica, *Polis, Revista de la Universidad Bolivariana,* 2003, vol. 1, núm. 4.
- CASTELLS, M., La Wikirevolución del jazmín, *La Vanguardia*, 29 de enero de 2011
- CAVOUKIAN, A. Privacy in the clouds. A White Paper on Privacy and Digital Identity: Implications for the Internet. *Information and privacy commissioner of Ontario*. 30 p
- CELIS QUINTAL, M.A., La protección de la intimidad como derecho fundamental de los mexicanos. En CIENFUEGOS SALGADO, D., y MACÍAS VÁZQUEZ, M.C. (Coords.), *Estudios en homenaje a Marcia Muñoz de Alba Medrano. Protección de la persona y derechos fundamentales*, Universidad Nacional Autónoma de México, 2006, p. 71-108, Disponible en web: http://www.bibliojuridica.org/libros/5/2253/9.pdf
- CERF. V., Internet Access Is Not a Human Right, *New York Times*, 4 de enero de 2012
- CHANG, H. Data protection regulation and cloud computing, En CHEUNG, A.S.Y. y WEBER, R.H. (eds). *Privacy and Legal Issues in Cloud Computing*. Elgar Publishing. 2015. 333 p.
- CHANG, V., WALTERS, R.J. y WILLS, G. *Delivery and Adoption of Cloud Computing Services in Contemporary Organizations*. IGI Global. Estados Unidos. 2015. 483 p.
- CHEN, D. y ZHAO, H. Data Security and Privacy Protection Issues in Cloud Computing, *2012 International Conference on Computer Science and Electronics Engineering*. 2012. Vol. 1. p. 647-651.
- CHERITON, D. Internet Arquitects Warn of Risks in Ultrafast Networks. *The New York Times*. 13 de noviembre de 2011.
- CHEUNG, A.S.Y. y WEBER, R.H. (eds). *Privacy and legal issues in Cloud Computing.* Edward Elgar Publishing. 2015.
- CIERCO, D (Coord.). Cloud computing: retos y oportunidades. *Fundación Ideas*. 2011.
- COLOM PLANAS, J.L. Cláusulas contractuales en entornos de cloud computing. 5 de octubre de 2012. Disponible en web: http://www.aspectosprofesionales.info/2012/10/clausulas-contractuales-en-entornos-de.html
- COLUMBUS, L., Roundup of Cloud Computing Forecasts and Market Estimates, 2016. *Forbes*. 13 de marzo de 2016.
- CONDE-POMPIDO TOURÓN, C. La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos (arts 588 sexies y 588 septies LeCrim), *Jornadas de Especialista en Criminalidad Informática*. 10 de marzo de 2016.
- CONRAD, I., DOVAS, M-U., POGGIOLLI, F., SELK, R., y WOLFGRAM, S. Cloud Computing Contracts – Discussion Paper on Subcontracting. *European Commission.* 25 de marzo de 2014.
- COOLEY, T.M., *A Treatise on the law of torts, or the wrongs which arise independently of contract*, Edited by J. Lewis, 3rd ed, Chicago: Callaghan & Company, 1906, 592 p.

- COSSROW. B.A, The Fig Leaf Precedent Set by *Stengart v. Loving Care Agency Inc*, *Technology Law, Bloomberg Law Repports*, 2010, vol 2, nº 10
- COTINO HUESO, L., Algunas claves para el análisis constitucional futuro de las libertades públicas ante las nuevas tecnologías (con especial atención al fenómeno de los «blogs»), en AA.VV. *Estudios jurídicos sobre la sociedad de la información y nuevas tecnologías*, Facultad de Derecho de Burgos, Burgos, 2005.
- COTINO HUESO, L., Las obligaciones del Estado: el nuevo derecho fundamental de acceso a internet y las garantías a partir de la redefinición de las clásicas libertades informativas, en AA.VV, *La responsabilidad del Estado por la utilización de las tecnologías de la información y la comunicación (TIC)*, Universidad Católica de Colombia, Bogotá, 2015, p. 51-94.
- COTINO HUESO, L. Algunas cuestiones clave de protección de datos en la nube. Hacia una «regulación nebulosa». *Revista Catalana de Derecho Público*. diciembre 2015, nº 51. p. 83-103.
- COVASSI, B. DSM Free Flow of Data Initiative and emerging issues of data ownership, access and usability. 5 de noviembre de 2015.
- CRESPO PÉREZ, S., El Cloud Computing explicado [en línea]. *Telos. Cuadernos de Comunicación e Innovación*. 2009. Disponible en web: https://telos.fundaciontelefonica.com/url-direct/pdf-generator?tipoContenido=articulo&idContenido=2009111912530001
- CUESTA SAINZ, C., ALONSO, J., TUESTA, D. y FERNÁNDEZ DE LIS, S. El desarrollo de la industria del cloud computing: impactos y transformaciones en marcha. *Observatorio de Economía Digital. BBVA Research.* 2014.
- DE ANDRÉS BLASCO, J., ¿Qué es Internet?; en GARCÍA MEXÍA, P.L, (Dir.), *Principios de Derecho de Internet*.
- DE BOER-BUQUICCHIO, M.,*Conférence sur l'éthique et les droits de l'homme dans la société de l'information,* Consejo de Europa, Estrasburgo, 13 de septiembre de 2007.
- DE CARRERAS SERRA, LL., *Régimen jurídico de la Información. Periodistas y Medios de Comunicación*, Ariel Derecho, 1996, 318 p.
- DE FILIPPI, P. y BELLI, L. Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation. *European Journal of Law and Technology.* 2012. Vol. 3. nº 2.
- DE HERT, P. y KLOZA, P., Internet (access) as a new fundamental right. Inflating the current rights framework?', *European Journal of Law and Technology*, 2012, Vol.3, nº 3.
- DELGADO KLOOS, C. y GARCÍA RUBIO, C., Historia de Internet; en CREMADES, J., FERNÁNDEZ ORDÓÑEZ, M.A, e ILLESCAS, R (Coords), *Régimen Jurídico de Internet*, La Ley-Actualidad, 2001, p. 87-100
- DELGADO MARTÍN, J., Derechos fundamentales afectados en el acceso al contenido de dispositivos electrónicos para la investigación de delitos, *Diario La Ley*, 29 de noviembre de 2013 nº 8202, Sección Doctrina.
- DELGADO MARTÍN, J. La prueba electrónica en el proceso penal. *Diario La Ley*. Nº 8167. Sección Doctrina, Año XXXIV. 10 Oct. 2013.

- DETERMANN, L. *Field Guide to Data Privacy Law*. Edward Elgar. 2nd ed. Cheltenham (UK), Northampton, MA, (USA). 2015. 232 p.
- DÍAZ REVORIO, J., *Los Derechos Humanos ante los nuevos avances Científicos y Tecnológicos. Genética e Internet ante la Constitución*, Derecho y tic's, Tirant lo Blanch, 2009.
- DÍAZ ROJO, J.A., Privacidad: ¿neologismo o barbarismo?, [en línea], *Espéculo, Revista de Estudios Literarios*, Julio-octubre 2002, nº 21. Disponible en Web: http://www.ucm.es/info/especulo/numero21/privaci.html, ISSN: 1139-3637
- DÍEZ-PICAZO, L.M., *Sistema de derechos fundamentales*, 1ª ed, Thomson-Civitas, 2003, 510 p.
- DOUKAS, C. y MAGLOGIANIS, I. Bringing IoT and Cloud Computing towards Pervasive [en línea]. *IMIS.* 2012. Disponible en web: https://pdfs.semanticscholar.org/4132/551dc6a891c62979c4f2c8a07f5d5cc90b6d.pdf?_ga=1.149196341.2024153542.1483012606
- DYSON, F.J. *The Sun, the Genome and the Internet*. Tools of Scientific Revolutions, The New York Public Library, Oxford University Press, 1999, 144 p.
- ECHEVERRI GARCÍA, E. El futuro está aquí: computación en nube. *Revista Sistemas.* 2008, nº. 108. p. 53-56.
- EISEMANN, T.R., PARKER, G. y VAN ALSTYNE, M. Opening Platforms: How, When and Why? *Harvard Business Review*. 31 de agosto de 2008.
- ETRO, F. The Economic Impact of Cloud Computing on Business Creation, Employment and Output in the E.U. An application of the Endogenous Market Structures Approach to a GPT innovation. *Review of Business and Economics*. 2009, 54(2), p. 179-208.
- FATÁS, J.M. y GARCÍA SANZ, F.J. Comentario al art. 5 del Reglamento de desarrollo de la LO 15/1999, de Protección de Datos de Carácter Personal. *Estudios y Comentarios Legislativos (Civitas)*. Editorial Aranzadi, SA, diciembre de 2008.
- FELICI, M. y FERNÁNDEZ GAGO, C. (eds). *Accountability and Security in the Cloud*. Springer. 2015. 306 p.
- FERNÁNDEZ, J.A. *Cloud computing*: ¡un futuro brillante! *NOTA ENTER. Instituto de Empresa*. nº 122. 17 de marzo de 2009.
- FERNÁNDEZ ALLER, C. Algunos retos de la protección de datos en la sociedad del conocimiento. Especial detenimiento en la computación en nube (cloud computing). *Revista de derecho UNED*. 2012. nº 10. p. 125-145.
- FERNÁNDEZ AVILÉS, J.A. y RODRÍGUEZ-RICO ROLDÁN, V., Nuevas tecnologías y control empresarial de la actividad laboral es España [en línea], *Labour&Law Issues* 2016, vol. 2, nº 1.
- FERNÁNDEZ ESTEBAN, M.L., El impacto de las nuevas tecnologías e Internet en los derechos del art. 18 de la Constitución, *Anuario de la Facultad de Derecho, Universidad de Extremadura*, 1999, nº 17, p. 523 a 544.
- FERNÁNDEZ ESTEBAN, M.L., La libertad de expresión en Internet, *Nueva Revista*, agosto 1999, nº 64.

- FERNÁNDEZ ESTEBAN, M.L., La regulación de la libertad de expresión en Internet en Estados Unidos y en la Unión Europea, *Revista de estudios políticos*, 1999, nº 103, p. 162 y ss.
- FERNÁNDEZ RODRÍGUEZ, J.J., Lo público y lo privado en Internet. Intimidad y libertad de expresión en la Red, *Instituto de Investigaciones Jurídica, Universidad Nacional Autónoma de México*, 2004. p. 95.
- FERNÁNDEZ SEGADO, F., La dinamización de los mecanismos de garantía de los derechos y de los intereses difusos en el Estado social. *Boletín Mexicano de Derecho Comparado, Biblioteca Jurídica Virtual*, 1995, nº 83, p. 563-597.
- FOURCADE, G. Seis variables para analizar antes de saltar a la nube. *IBM.* 2011.
- FREY, S., LUTHJE, C., y REICH, C. Key Performance Indicators for Cloud Computing SLAs. *IARIA.* 2013. p. 60-64.
- FROSINI. V., *Informática y Derecho*, traducción del italiano de GUERRERO, J. y AYERRA REDIN, M., Bogotá, Themis, 1988, 179 p.
- GARCÍA DE ENTERRÍA, E., Reflexiones sobre la Ley y los Principios Generales del Derecho, Revista de Administración Pública, Enero-abril 1963, nº 40, p. 189-222.
- GARCÍA DEL POYO, R. Cloud Computing: Aspectos jurídicos clave para la contratación de estos servicios. *reri.difusionjuridica.es*. p. 48-91.
- GARCÍA MEXÍA, P.L., Derechos y libertades, internet y tics, Valencia, Tirant lo Blanch, 93 p., internet y tic'
- GARCÍA MEXÍA, P.L., *Derecho Europeo de Internet*, Netbiblo, 2009, 279 p.
- GARCÍA MEXÍA, P. Cloud computing. Sus implicaciones legales. Revista Aranzadi de derecho y nuevas tecnologías. 2010, nº 23, p. 79-88.
- GARCÍA MEXÍA, P.L., *Historias de Internet. Casos y cosas de la red de redes*, Valencia: Tirant Humanidades, 2012, 167 p.
- GARCÍA MEXÍA, P. Cloud Computing. Sus dilemas legales. *Universidad Politécnica de Madrid*.
- GARCÍA MEXÍA, P. Internet y derecho en la era del cloud computing. *Blog La Ley en la Red*. 10 de febrero de 2014.
- GEAMBASU. R, GRIBBLE, S.D. y LEVY, H.M., CloudViews: Communal Data Sharing in Public Clouds. *Proc. Workshop Hot Topics in Cloud Computing (HotCloud).* 2009, article 14.
- GELERNTER, D. *Mirror Worlds Or the Day Software Puts the Universe in a Shoebox...How It Will Happen and What It Will Mean*. 1st ed. Oxford University Press. 1992. 256 p.
- GELLMAN, R. Privacy in the Clouds: Risk to Privacy and Confidentiality from Cloud Computing. *World Privacy Forum*. 23 de febrero de 2009.
- GIANNAKOURIS, K. y SMIHILY, M. Cloud computing - statistics on the use by enterprises. *Eurostat.* November 2014.
- GLEESON, N.C. y WALDEN, I. It's a jungle out there'?: Cloud computing, standards and the law. *European Journal of Law and Technology*. Nov. 2014. Vol. 5. nº 2.
- GOLDEN, B. The Death of the SLA*. CIO FROM IDG.* 17 de febrero de 2015.
- GOMES, L. y BULEY, T. The Death of the PC. *Forbes.* 2009, Vol. 194, número 12.

- GÓMEZ SÁNCHEZ, Y., La protección de los datos genéticos: el derecho a la autodeterminación informativa, *Derecho y Salud*, vol. 16, nº extra 1, 2008 (Ejemplar dedicado a: XVI Congreso "Derecho y Salud"), p. 59-78.
- GÓMEZ SÁNCHEZ, Y*., Derecho Constitucional Europeo: derechos y libertades*, 1ª ed., Madrid: Sanz y Torres, 2005, 499 p.
- GONG, C., LIU, J., ZHANG, Q, CHEN, H, y GONG, Z. The Characteristics of Cloud Computing. *39th International Conference on Parallel Processing Workshops*. 2010. P. 275-279.
- GONZÁLEZ, D. y RILO, J. *Cloud Computing* y seguridad. *XII Reunión Española sobre Criptología y Seguridad de la Información (RECSI 2012).* 2012.
- GONZÁLEZ ÁLVAREZ, R., Aproximación a los derechos de cuarta generación, Disponible en Web: www.tendencias21.net/derecho/attachment/113651/
- GONZÁLEZ-CALERO MANZANARES, F.R. Primera aproximación al Reglamento General de Protección de Datos. *Elderecho.com*. 28 de enero de 2016.
- GORMLEY, K., One hundred years of privacy*, Wisconsin Law Review,* University of Wisconsin, 1992, nº 1335, p. 1335-1441.
- GRAEF, I. Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union. *Telecommunications Policy 2015*. Vol. 39, No. 6. p. 502-514.
- GRAHAM, M. y DUTTON, W.H. *Society and the Internet. How Networks of Information and Communication are Changing Our Live*. Oxford University Press 2014. 416 p.
- GRINGAS, C. UK Cloud Computing Interception - nothing new. *Olswang*. 2011.
- GUASCH PORTAS, V. y SOLER FUENSANTA, J.R. Cloud Computing, cláusulas contractuales y reglas corporativas vinculantes. *Revista de Derecho UNED.* 2014. nº 14. p. 247-269.
- GUDE FERNÁNDEZ, A., La videovigilancia laboral y el derecho a la protección de datos de carácter personal, *Revista de derecho político*, 2014, nº 91, p. 43-90.
- GUISSASOLA LERMA, C., Menores, intimidad y riesgos de la Sociedad tecnológica: el caso particular del sexting, en FAYOS GARDÓ, A., (Coord.), *Los derechos a la intimidad y a la privacidad en el siglo XXI,* Dykinson, 2015, p. 114
- GUTWIRTH, S. POULLET, Y. HERT, P. y LEENES R. *Computers, Privacy and Data Protection: an Element of Choice.* Springer. 2011. 482 p
- HANSEN, M. The Art of Intervenability for Privacy Engineering. *Workshop "Data Protection, Privacy, and Transparency*" (DPPT'15). Hamburg. 26 de mayo de 2015.
- HENRIQUES, M. y DIGN, J. Purging the Cloud: Data Destruction in the Age of Cloud Computing. *Womble Carlyle*. 23 de junio de 2014.
- HON, K. W., MILLARD, C. y WALDEN, I. Negotiating Cloud Contracts: looking t clouds from both sides now. *Stanford Technology Law Review.* Fall 2012. Vol. 16. Nº 1. p. 79-129.
- HON, K.W, MILLARD, C. y MILLARD, C. Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the Eea? The Cloud of Unknowing, Part 4. *SCRIPTed*. abril 2012. Vol 6. Issue 1. p. 25-63.

- HON, K.W., HÖRNLE, J. y MILLARD, C. Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing. *International Review of Law, Computers & Technology*. 2012, vol. 26, Iss. 2-3, p. 129-164.
- HON, K. Data protection and service providers - new obligations, liabilities and contract changes loom. *Pinsent Masons*, 7 de septiembre de 2015.
- HON, W.K. GDPR: Killing cloud quickly? *International Association of Privacy Professionals (IAPP).* 17 de marzo de 2016,
- HUSTINX, P. Data protection and Cloud Computing under EU law. *Third European Cyber Security Awareness Day.* 13 April, 2010.
- IOKOMONOU, D. (ENISA). Impact of the proposed data protection regulation on cloud computing. *CSP Forum.* 28 y 29 de abril de 2015.
- JANSEN, W. y GRANCE, T., Guidelines on Security and Privacy in Public Cloud computing. *National institute of Standards and Technology* (*NIST*), *U.S. Department of Commerce.* Diciembre de 2011.
- JONES, T. La anatomía de un hipervisor Linux [en línea]. *IBM Developer Works.* 31 de mayo de 2009.
- JOYANES AGUILAR, La Computación en Nube (Cloud Computing): El nuevo paradigma tecnológico para empresas y organizaciones en la Sociedad del Conocimiento. *Icade. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales*. enero-abril 2009, nº 76, p. 95-111.
- JOYANES AGUILAR, L. Computación en la nube e innovaciones tecnológicas. El nuevo paradigma de la Sociedad del Conocimiento [en línea]. *Grupo de Investigación de Ingeniera del Software y Sociedad de la Información y del Conocimiento*. Disponible en web: https://gissic.files.wordpress.com/2011/07/computacion_en_nube_revista_paraguay_luis_joyanes.pdf
- KAMAINOU, D., MILLARD, C. y KUAN HON, W. Privacy in the Clouds: an Empirical Study of the Terms of Service and Privacy Policies of 20 Cloud Service Providers*. Queen Mary University of London. School of Law Legal Studies Research Paper No 209/2015*. 2015. 71 p.
- KAMBELLARI, E., Employee email monitoring and workplace privacy in the European perspective, *Iustinianus Primus Law Review*, 2014, nº 8, p. 1-18.
- KESIDIS, G., URGAONKAR, B., NASIRIANI, N. y WANG, C. Neutrality in Future Public Clouds: Implications and Challenges*. 8th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 16),* USENIX Association. Denver, Colorado. 2016.
- KISSEL, R., REGENSCHEID, A, SCHOLL, M. y STINE, K. Guidelines for Media Sanitization. *National Institute of Standards and Technology*. Diciembre de 2014.
- KOKOTT, J. y SOBOTTA, C., The distinction between privacy and data protection in the jurisprudence of the CJEU and the EctHR, *International Data Privacy Law*, 2013, vol. 3, nº. 4, p. 222-228.

- KSHETRI, N. Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Journal Telecommunications Policy archive*. mayo de 2013. Vol. 37. p. 372 a 386.
- KUNER, C. Data Protection and Cloud Computing: an Overview of the Legal Issues. *Nordic IT Law Conference*. Copenhagen.12 November 2010.
- LA RUE F., *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Nueva York, Naciones Unidas, 16 de mayo de 2011, 22 p. Disponible en Web. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
- LAPORTA SAN MIGUEL, F.J., El concepto de derechos humanos, *Doxa. Cuadernos de Filosofía del Derecho*, 1987, nº 4.
- LASPROGATA, G., KING, N., y PILLAY, S., Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada, *Stanford Techonology Law Review*, 2004, nº 4.
- LAUDATI, L., Summaries of EU Court Decisions relating to data protection 2000-2015, *European Anifraud Office,* 28 january 2015. Disponible en web: https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf
- LE GRAND, G. Cloud computing and personal data protection. *CSA Congress EMEA*. noviembre de 2015. Disponible en web: https://csacongress.org/wp-content/uploads/2015/11/csa-congress-emea-2015_-_Gwendal-Grand.pdf
- LEATHERMAN, B., Internet Censorship and the Freedom of Speech, American University, Washington D.C., 19 de mayo de 1999, Disponible en web: http://www.szasz.com/undergraduate/leathermanpaper.htm
- LESSIG, L. *The Arquitecture of Privacy*, *TaiwanNet* 98, Taipei, 1998, 23 p
- LEVINSON, A.R., Industrial Justice: Privacy Protection for the Employed, *Cornell Journal of Law and Public Policy,* 2009, vol 18, p. 609-688
- LEVNISON, A.R., Toward a cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees, *West Virginia Law Review*, vol. 114 2011, p. 461-550.
- LICKLIDER, J.C.R. *Memorandum for: Members and Affiliates of the Intergalactic Computer Network* [en línea]. 23 de abril de 1963. Disponible en web: http://worrydream.com/refs/Licklider-IntergalacticNetwork.pdf
- LIMA TORRADO, J., Ciberespacio y protección de los derechos: ¿hacia una cibercultura de los derechos humanos?, *Cuadernos electrónicos de Filosofía del Derecho* [en línea], 2002, nº 5, Disponible en web: http://www.uv.es/CEFD/5/lima.html, I.S.S.N.: 1138-9877
- LINDSAY, A.F., y JEFFERIES, T.R., *French court limits the scope of employee data protection*, 2013. Disponible en web: http://www.lexology.com/library/detail.aspx?g=0b1abe79-8a71-4625-b43a-f40b58c27673
- LÓPEZ CARBALLO, D.A. (Coord.), *Protección de datos y habeas data: una visión desde Iberoamérica*, Agencia Española de Protección de Datos, 2015, 218 p.

- LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa*. Temas Clave de la Constitución española, Tecnos, 1990. 207 p
- LUCAS MURILLO DE LA CUEVA, P. y PIÑAR MAÑAS, J.L., *El derecho a la autodeternimación informativa*, Madrid, Fundación coloquio jurídico europeo, 2009, 180 p.
- LUCAS MURILLO DE LA CUEVA, P., La construcción del derecho a la autodeterminación informativa, *Revista de estudios políticos*, 1999, nº 104, p. 35-60.
- LUCENA CID, I.V., La protección de la intimidad en la era teconlógica: hacia una reconceptualización, *Revista internacional de pensamiento político* [en línea], 2012, nº. 7, p. 117-144. Disponible en web: http://rabida.uhu.es/dspace/bitstream/handle/10272/7843/la_protecci%C3%B3n_de_la_intimidad.pdf?sequence=2 ISSN 1885-589X
- MACOVEI, M., *Freedom of expression. A guide to the implementation of article 10 of the European Convention of Human Rights*, 2nd edition, Consejo de Europa, 2004, 65 p. Human Rights Handbook, nº 2.
- MAILLAND, J., Freedom of Speech, the Internet, and the Costs of Control: The French Example, New York University Journal of International Law & Politics, Summer 2001, Vol. 33, nº 4, p. 1179-1234.
- MANTELERO, A. Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution [en línea]. *European Journal for Law and Technolo*gy. 2012. vol. 3, nº. 2. Disponible en web: http://ejlt.org/article/view/96/253
- MARTÍNEZ DE VELASCO FARINOS, A., Los orígenes de Internet; en AA.VV. *Las Ciencias Sociales en Internet*, Mérida, Junta de Extremadura, 2001, p. 22.
- MARTÍNEZ MARTÍNEZ, R., El derecho fundamental a la protección de datos: perspectivas, *IDP: revista de Internet, derecho y política = revista d'Internet, dret i política* [en línea], 2007, nº 5. Disponible en web: http://www.uoc.edu/idp/5/dt/esp/martinez.pdf, ISSN-e 1699-8154.
- MARZO PORTERA, A.M. Privacidad y cloud computing, hacia dónde camina Europa. Revista de Sociales y Jurídicas. 2012. Vol. 1. nº 8. p. 202-229.
- MAQUEO RAMÍREZ, M.S., MORENO GONZÁLEZ, J. y RECIO GAYO, M. *Lineamientos de Protección de Datos en el Cómputo en la Nube: Parámetros para su elaboración*. Centro de Investigación y Docencia Económicas. México. septiembre de 2014. 79 p.
- MATITEYAHU, T., Drone Regulations and Fourth Amendment Rights: The Interaction of State Drone Statutes and the Reasonable Expectation of Privacy, *Columbia Journal of Law and Social Problems*, Winter2015, Vol. 48 Issue 2, p. 265-307
- MATUS ARENAS, J. Transferencias internacionales a países con niveles adecuados y no adecuados de protección. Aspectos prácticos. *Seminario Regional de Protección de Datos*. Montevideo, Uruguay. 1 a 4 de junio de 2010.
- MAXWELL, W. y WOLF, F.CH. A Global Reality: Governmental Access to Data in the Cloud A comparative analysis of ten international jurisdictions*. A Hogan Lovells White Paper.* Disponible en web: http://www-05.ibm.com/ch/services/documents/sce/br-government-access-to-cloud-data.pdf

- MAXWELL, W. y WOLF, F.CH. A Global Reality: Governmental Access to Data in the Cloud A comparative analysis of ten international jurisdictions. *A Hogan Lovells White Paper*. Disponible en web: http://www-05.ibm.com/ch/services/documents/sce/br-government-access-to-cloud-data.pdf
- McGRAW SWAMINATHA, T. y NEFF, K. Microsoft-Ireland: Decision underscores tension between privacy principles and the digital environment. *DLA Pipper*. 19 de junio de 2016.
- MEGÍAS QUIRÓS, J.J., Privacidad e internet: intimidad, comunicaciones y datos personales, *Anuario de derechos humanos*, 2002, nº. 3, p. 515-560.
- MELL, P. y GRANCE, T. Effectively and Securely Using the Cloud Computing Paradigm. *NIST, Information Technology Laboratory*. 2009.
- MELL, P. y GRANCE, T., The NIST definition of Cloud computing (Draft), Recommendations of the National institute of Standards and Technology. *National institute of Standards and Technology (NIST), Special-Publication,* Enero 2011.
- MENON, G. Regulatory Issues in Cloud Computing -An Indian Perspective. *Journal of Engineering, Computers & Applied Sciences (JEC&AS)*. July 2013, vol. 2, nº 7. p. 18-22.
- McGILLIVRAY, K. A right too far? Requiring cloud service providers to deliver adequate data security to consumers. *International Journal of Law and Information Technology*. 2016. nº 25. p. 1-25.
- MILLER, R. y WHITTEN, T. Subcontratación segura en la nube: cinco preguntas clave que hay que formular. *CA Technologies.* 2012.
- MIRALLES, R. Cloud computing y protección de datos. Revista de Internet, Derecho y Política. 2010. nº 11. p. 14-23.
- MIRALLES R., El derecho a la portabilidad de los datos personales. Abogacía. 15 de noviembre de 2012.
- MIRALLES, R. El derecho a la portabilidad de los datos personales o prestaciones "premium" del tradicional derecho de acceso; en VALERO TORRIJOS, J. *La protección de datos personales en internet ante la innovación tecnológica riesgos, amenazas y respuestas desde la perspectiva jurídica.* Aranzadi. 2013. p. 273 a 290.
- MONTERO, S. Cumplimiento, seguridad y control en la nube ¿Es posible? *Blog KPMG Ciberseguridad*. 6 de junio de 2015.
- MUELLER, M.L., *Networks and States. The Global Politics of Internet Governance*, The MIT Press, 2010, 320 p
- MURAKAMI, T. y FURIYUMA, A. Ubiquitous Networking: Towards a New Paradigm. *Nomura Research Institute Papers*. 2001, nº 2, p. 1-7.
- NARAYANAN, V. Harnessing the Cloud: International Law. Implications of Cloud-Computing. *Chicago Journal of International Law*, 2012, vol. 12, nº 2, p. 783-809.
- NAVAS NAVARRO, S. Computación en la nube: Big Data y protección de datos personales. *InDret* 4/2015. p. 1-48.

- NISSENBAUM, H., Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*, 1998, vol. 17, p. 559-596. Disponible en web: https://pdfs.semanticscholar.org/307f/83f933ae0c4e53392b7c0046d3dc24e2e4f3.pdf
- NOBLE FOSTER, T. Navigating Through the Fog of Cloud Computing Contracts. *J. Marshall J. Info. Tech. & Privacy*. 2013. Vol. 30. Issue 1. p. 13-30.
- NÚÑEZ ENCABO, M., Europa y EE.UU: dos conceptos divergentes de la libertad de expresión, *Anuario de Derechos Humanos, Nueva Época*, 2008, Vol. 9, p. 461-478
- OROZCO PARDO G. y MORENO NAVARRETE, M.A. El contrato en el contexto de la unificación del Derecho Privado. *Anales del Derecho.* 2011, nº 29. p. 115-160.
- ORTIZ DE SOLÓRZANO AURUSA, C., Facultades empresariales de control, tics y privacidad del trabajador, *Revista Aranzadi de derecho y nuevas tecnologías*, 2015, nº 37, p. 41-72.
- ORZA LINARES, R.M., ¿Es posible la creación de nuevos derechos fundamentales asociados a las nuevas tecnologías de la información y de la comunicación?, En: a*ctas del IV Congreso Online del Observatorio para la Cibersociedad,* celebrado online del 12 al 29 de noviembre de 2009.
- OTTO, M., *The Right to Privacy in Employment: A Comparative Analysis,* Bloomsbury Publishing*,* 2016, 256 p.
- PATRIKIOS, A. Getting to know the GDPR, Part 2 – Out-of-scope today, in scope in the future. What is caught? [en línea]. *Privacy and Information Law Blog*. 20 de octubre de 2015. Disponible en web: http://privacylawblog.fieldfisher.com/2015/getting-to-know-the-gdpr-part-2-out-of-scope-today-in-scope-in-the-future-what-is-caught
- PAVEL BURLOJU, M. *Cloud computing and the regulatory framework for telecommunications and information society services*. Tilburg University. febrero de 2012.
- PITT-PAYNE, T., Data Protection the EU Reform Proposals [en línea], *kbw*, 22 de febrero de 2012. Disponible en web: http://www.11kbw.com/uploads/files/DPTPPP.pdf p. 2
- PEARSON, S. y CHARLESWORTH, A. Developing accountability-based solutions for data privacy in the cloud*";* en FRIEDWALD, M. y POHORYLES, R.J. (Eds.). *Privacy and Security in the Digital Age: Privacy in the Age of Super-Technologies.* Routledge. 2016. p. 7-35.
- PECES-BARBA MARTÍNEZ, G., Los derechos fundamentales de naturaleza política y las nuevas tecnologías, en AA.VV., *Parlamento y nuevas tecnologías, II Jornadas parlamentarias de la Asamblea de Madrid*, Asamblea de Madrid, octubre 2001, p. 151 a 159.
- PEREZ LUÑO, A.E., Las generaciones de derechos humanos, *Revista del Centro de Estudios Constitucionales*, Septiembre-Diciembre 1991, nº 10, p. 203-217
- PÉREZ LUÑO, A.E., *Los derechos fundamentales*, 5ª edición, Tecnos, 1993, Temas Clave de la Constitución Española, 240 p.
- PÉREZ LUÑO, A.E., Impactos sociales y jurídicos de Internet, *Argumentos de razón técnica: Revista española de ciencia, tecnología y sociedad, y filosofía de la tecnología* [en línea], 1998, Nº 1, p. 33-48. Disponible en Web: http://www.argumentos.us.es/numero1/bluno.htm ISSN 1139-3327
- PEREZ LUÑO, A.E, Internet y los derechos humanos, *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento* [en línea], 2002, nº 2, Facultad de Derecho,

Universidad de Huelva, p. 101-121, Disponible en web : http://www.uhu.es/derechoyconocimiento/DyC02/DYC002_A05.pdf

- PÉREZ LUÑO, A.E., Nuevas tecnologías, informática y Derecho, en ASIS, R.D., BONDÍA, B., y MAZA, E., (coords.), *Los desafíos de los derechos humanos hoy*, Dykinson, 2007, p. 487-508.
- PÉREZ LUÑO, A.E., Bioética e intimidad. La tutela de los datos personales biomédicos, en *Bioética y derechos humanos*, Ana María Marcos del Cano (coord..), Universidad Nacional de Educación a Distancia, 2011, p. 77-104.
- PETERSEN, T. y ESCHE, A., Perserving an Old Model in the New World: German Economic Policy [en línea], *Newpolitik,* octubre 2016. Disponible en web: http://www.bfna.org/sites/default/files/publications/Echoes_of_history_Understanding_German_Data_Protection_Freude.pdf
- PIZZORUSSO, A., Las generaciones de derechos, traducido por BERZOSA LÓPEZ, D., *Anuario Iberoamericano de Justicia Constitucional*, 2001, nº 5.
- POHLMANN, N., REIMER, H. SCHNEIDER, W. ISSE 2010 Securing Electronic Business Processes Springer Science & Business Media. 2011. 213 p.
- POLLICINO, O., European Judicial Dialogue and the Protection of Fundamental Rights in the New Digital Environment: An Attempt at Emancipation and Reconciliation, en MORANO-FOADI, S. y VICKERS L. (eds.), *Fundamental Rights in the EU: A Matter for Two Courts*, Blomsbury, 2015, p. 93-114.
- POST, D.G., *In Search of Jefferson´s Moose: Notes on the State of Cyberspace*, Oxford University Press, 2009, 244 p.
- PRIETO HERGUETA, J. Transferencias internacionales de datos: las garantías de las normas corporativas vinculantes (BCR). *7ª Sesión Anual Abierta de la AEPD*. 21 de abril de 2015.
- PROUST, O. Article 29 Working Party issues draft model clauses for processor-to-subprocessor data transfers. *Privacylawblog*. 9 de abril de 2014.
- PUYOL MONTERO, J. *Algunas consideraciones sobre Cloud Computing*. Agencia Española de Protección de Datos. Agencia Estatal Boletín Oficial del Estado. Madrid. 2013. 273 p. RAMOS ROMEU, F., *Data Protection in the ECHR`s case law*,
- RAYPORT, J.F. y HEYWARD, A. Envisioning the Cloud: The Next Computing Paradigm [en línea]. *Marketspace.* 20 de marzo de 2009.
- REED, C., *Internet Law*, 2nd Ed, Cambridge University Press, 2004, 374 p.
- REIDENBERT, J.R., Privacy in Public, *University of Miami Law Review,* 2014, vol. 69, p. 141-160.
- REINGOLD, B., MRAZIK R. y D'JAEN, M. Cloud Computing: Whose Law Governs the Cloud? (Part III). *Cyberspace Lawyer.* January-February 2010, p. 1-6.
- RENDA, A. Competition, Neutrality and Diversity in the Cloud. *Digiworld Economic Journal.* 2012. nº 85.
- RIBAS, J. La subcontratación en el cloud computing. Expansión. 24 de mayo de 2012.
- RODRÍGUEZ MARCA, E., El derecho fundamental a la protección de datos de carácter personal en Venezuela y su desarrollo desde la Sala Constitucional del Tribunal Supremo de Justicia [en

línea] Red Iberoamericana de protección de datos. 15 de septiembre de 2015. Disponible en web: http://www.redipd.org/noticias_todas/2015/tribuna/news/15_09_2015-ides-idphp.php

- ROHRMANN, C.A. y ROCHA CUNHA, J.F.S., Some legal aspects of Cloud Computing Contracts. *Journal of International Commercial Law and Technology.* 2015, vol. 10, nº. 1. p. 37-45.
- RUBÍ NAVARRETE, J. El proveedor de cloud como encargado del tratamiento, en MARTÍNEZ MARTÍNEZ, R (Ed.). *Derecho y Cloud Computing.* Thomson Reuters. 2012. p. 87 a 107.
- RUBIO MORAGA, A.L., Censura en la Red: restricciones a la libertad de expresión en Internet; en SANZ ESTABLÉS, C., SOTELO GONZÁLEZ, C. RUBIO MORAGA, A.L (Coords.), *Prensa y periodismo especializado II*, 2004, p. 597-607.
- RUIZ MIGUEL, C., La tercera generación de derechos fundamentales, *Revista de Estudios Políticos*, abril-junio, 1991, nº. 72, p. 301 y ss.
- SAINZ MORENO, F. Conceptos jurídicos indeterminados, interpretación y discrecionalidad administrativa. Civitas, Madrid. 1976. 364 p.
- SAIZ PEÑA, C.A. Medidas de seguridad en el Cloud Computing; en MARTINEZ MARTINEZ, R. (ed). Derecho y cloud computing. Thomson Reuters. Civitas. 2012. p. 149-178.
- SALAS CLAVER, G. Algunos apuntes jurídicos sobre los contratos en Cloud Computing. Abril de 2013. Disponible en web: http://www.securitybydefault.com/2013/04/algunos-apuntes-juridicos-sobre-los_9.html
- SAMANI, R., REAVIS, J. y HONAN, B. *CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security*. Elsevier. USA, 2015. 236 p.
- SANCHO VILLA. D. Negocios internacionales de Tratamiento de datos personales", Thomson Reuters, Civitas, Cizur Menor. 270 p.
- SANZ LARRUGA, F.J., El Derecho ante las nuevas tecnologías de la información, *Anuario da Facultade de Dereito da Universidade da Coruña*, 1997, nº 1, p. 506 y ss.
- SEGOVIANO ASTABURUAGA, M.L., El difícil equilibrio entre el poder de dirección del empresario y los derechos fundamentales de los trabajadores [en línea], *Revista jurídica de Castilla y León*, 2004, nº 2, p. 147-190.
- SEN, J. Security and Privacy Issues in Cloud Computing. *Architectures and Protocols for Secure Information Technology Infrastructures*. 2013. p. 1-42.
- SERRERA COBOS, P. *Cloud Computing* y protección de datos. *Dintel*. 2010. p. 182-184.
- SCHELLEKENS, B.J.A. The European Data Protection Reform in the light of cloud computing. *Tilburg University*. 2013. 79 p.
- SCHUPPERT, S. German DPAs Issue Rules for Cloud Computing Use. *Chronicle of Data Protection. Hogan Lovells.* 13 de octubre de 2011.
- SERRERA COBOS, R. Cloud Computing y protección de datos. *Revista Dintel*. junio 2010. p. 182-184.
- SIDLEY, *Essentially Equivalent. A comparison of the legal orders for privacy and data protection in the European Union and United States*, January 2016, 173 p., Disponible en web: http://www.sidley.com/~/media/publications/essentially-equivalent---final.pdf

- SMITH. B, Building Confidence in the Cloud: A Proposal for Industry and Government Action for Europe to Reap the Benefits of Cloud computing. *European Commission. Contribution by Microsoft.* Bruselas, enero de 2010.
- SMOLLA R.A., *First Amendment Law Handbook*, Thomson-Reuters, 2014-2015, 628 p.
- SOLOVE, D.J., Conceptualizing Privacy, *California Law Review,* vol. 90, issue 4, article 2, 2002, p. 1087-1155. Disponible en web: http://scholarship.law.berkeley.edu/californialawreview/vol90/iss4/2
- SOSINSKY, B. *¿Qué es la nube? El futuro de los sistemas de información.* Anaya, 2012. 591 p.
- STUTZMAN, K. Data Destruction – Protecting private data when moving to or from a cloud service. *Ongoing Operations.* 2012.
- SULLIVAN, B., *Privacy lost: Does anybody care?,* Disponible en web: http://www.msnbc.msn.com/id/15221095/print/1/displaymode/1098/
- SULLIVAN, B., *La difference' is stark in EU, U.S. privacy laws*, Disponible en web: http://www.msnbc.msn.com/id/15221111/ns/technology_and_science-privacy_lost/
- SWARTZ, M.J. *Are* You Ready For An FBI Server Takedown? *Network Computing*. 7 de enero de 2011.
- SCHWARTZBERG, S., Hacking the fourth: how the gaps in the law and fourth amendment jurisprudence leave the right to privacy at risk, *University of La Verne Law Review*¸ abril 2009, vol. 30, p. 467-494.
- TEJADA DE LA FUENTE, E. Apuntes sobre la reforma procesal en materia de investigación tecnológica. *Revista de Privacidad y Derecho Digital*. Abril 2016. Nº 3. p. 181-190.
- TEMPERINI, M.G.I. Propiedad Intelectual: La cesión de licencias como elemento esencial en los Servicios Cloud Computing. *Jornadas Argentinas de Informática Nº 40 (JAIIO 40) - Simposio de Informática y Derecho*. 2011.
- TIKK-RINGAS, E., SPIRITO, C., HUSAIN, A. y AL-TAYEB, I. Considerations for regulatory and policy approaches to Cloud Computing in the GCC. *IISS White Paper.* 2013.
- THOMPSON, R.M., Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses, *Congressional Research Service*, 2013. Disponible en web: https://fas.org/sgp/crs/natsec/R42701.pdf
- TREACY, B. Working Party confirms 'controller' and 'processor' distinction. *Privacy&Data Protection*. Vol. 10, Issue 5. p. 3-5.
- VAN EECKE, P. Cloud Computing: Legal Issues. *DLA Pipper*. Disponible en web: http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/DLA_Cloud%20computing%20legal%20issues.pdf
- VAQUERO, L.M., RODERO-MERINO, L., CÁCERRES, J. y LINDER, MAIK. A Break in the Clouds: Towards a Cloud Definition. *Computer Communication Review.* enero de 2009, Vol. 39, nº 1. ftp://doc.nit.ac.ir/cee/jazayeri/research%20method/a%20break%20in%20the%20*cloud*s%20towards%20a%20*cloud*%20definition.pdf
- VELASCO NUÑEZ, E. Aspectos procesales de la investigación y de la defensa en los delitos informáticos. Ilustre Colegio de Abogados de Madrid. Disponible en web:

http://web.icam.es/bucket/Aspectos%20Procesales%20de%20la%20Investigacion%20y%20Defensa%20Delitos%20Informaticos.pdf

- VELAZQUEZ YANEZ, H. Paso a paso: Destrucción de soportes y documentos conforme a la normativa de protección de datos personales. *www.legaltoday.com* 27 de febrero de 2016.
- VERA SANTOS, J.M., Derechos fundamentales, Internet y nuevas tecnologías; en Pablo García Mexía (coord..), *Principios de Derecho de Internet*, 1ª edición, Tirant lo Blanch, 2005, p. 189-246.
- VINCENT, M. y HART, N. Cloud Computing-Legal Issues in the Cloud. Truman Hoyle Lawyers. *Mondaq*. 26 de octubre de 2010.
- VINCENT, M. y HART, N. Cloud Computing-Legal Issues in the Cloud. *Journal for the Australian and New Zealand Societies for Computers and the Law.* January 2011, nº 79, p. 1-6.
- VILLARINO MARZO, J., La Unión Europea ante los retos de la era digital. La reforma de la política europea de protección de datos, en PASCUA MATEO, F. (Dir.), *Derecho de la Unión Europea y el Tratado de Lisboa*, Dykinson, 2013, p. 561-597.
- VILLARINO MARZO, J. Privacidad desde el diseño en la propuesta de reglamento europeo de protección de datos. *Revista Aranzadi de derecho y nuevas tecnologías*, ISSN 1696-0351. 2013. Nº. 32. p. 45-68.
- VILLAVERDE MENÉNDEZ, I., Nuevas tecnologías, videovigilancia, derecho a la protección de datos y ficheros policiales, *Revista Catalana de Seguridad Pública,* 2006, nº 16, p. 177 a 202. Disponible en web: http://www.raco.cat/index.php/rcsp/article/viewFile/130221/179659
- WAGLE, S.S., Cloud Computing Contracts: Regulatory Issues and Cloud Providers' Offer: An nalysis. *Research Work. University of Luxembourg.* Disponible en web: http://www.ifip-summerschool.org/wp-content/uploads/2016/08/IFIP-SC-2016_pre_paper_11.pdf
- WALDEN, I. Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent. *Queen Mary, University of London Cloud legal Project*. 14 de noviembre de 2011.
- WALLACH, S., The Medusa Stare: Surveillance and Monitoring of Employees and the Right to Privacy, *International Journal of Comparative Labour Law and Industrial Relations*, 2011, p. 189-219.
- WARREN, S.D. y BRANDEIS, L.D., The Right to Privacy*, Harvard Law Review*. December 15, 1890, Vol IV, nº 5, p. 193-220.
- WEST, P. Saving Money Through Cloud Computing. *Governance Studies*. The Brookings Institutions, Washington. 2010.
- WINGFIELD, N. y KANG, C. Microsoft Wins Appeal on Overseas Data Search. *New York Times*. 14 de julio de 2016.
- WILHELM, E.O., A brief history of the General Data Protection Regulation. Disponible en web: https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/
- WHITMAN, J.Q., The Two Western Cultures of Privacy: Dignity versus Liberty, *Yale Law Review*, marzo 2004, p. 1151 a 1221.
- WU, T., Network Neutrality, Broadband Discrimination, *Journal on telecom and high tech law*, 2003, vol. 2, p. 141-179.

- WU, T., Why everyone was wrong about Net Neutrality?, *New York Times*, 26 de febrero de 2015.
- YAZIR, Y.O, MATTHEWS, C., FARAHBOD, R., NEVILLE, S., GUITOUNI, A. GANTI, S., COAD, Y., Dynamic Resource Allocation in Computing Clouds using Distributed Multiple Criteria Decision Analysis. In: Proceeding of IEEE 3rd International Conference on Cloud Computing. 2010. p. 91–98.
- YIGIBASIOGLU, O.M., MACKENZIE, K. y LOW, R. Cloud Computing: How does it differ from IT outsourcing and what are the implications for practice and research? *The International Journal of Digital Accounting Research*. 2013. nº 13. p. 99-121.
- YOUSEFF, L., BUTRICO, M., y DA SILVA, D. Toward a Unified Ontology of Cloud Computing*. Grid Computing Environments Workshop*. 2008.
- ZALAZAR, A.S., GONNET, S. y LEONE, H. Aspectos Contractuales de Cloud Computing. *Tercer Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática (CIIDDI)*. Mar del Plata, Argentina. 2014.
- ZEITER, A. The New General Data Protection Regulation of the EU and its Impact on IT Companies in the U.S. Transatlantic Technology Law Forum, A joint initiative of Stanford Law School and the University of Vienna School of Law. *TTLF Working Papers.* 2014, nº 20. p. 1-30.
- ZITTRAIN, J. Lost in the Cloud*. New York Times.* July 20th, 2009.

JURISPRUDENCIA

TJUE

- Tribunal de Justicia de la Unión Europea. Caso Lindquist. Sentencia de 6 de noviembre de 2003.
- Tribunal de Primera Instancia (Gran Sala). Caso Microsoft Corp (T-201/04).
- Tribunal de Justicia de la Unión Europea (sala tercera). Caso *Nikolaou vs. Comisión Europea*. Sentencia de 12 de septiembre de 2007.
- Tribunal de Justicia de la Unión Europea. Caso Tietosujavaltuutettu c. Satakunnan Markkinapörssi Oy y otros (C 73/07), Sentencia de 16 de diciembre de 2008.
- Tribunal de Justicia de la Unión Europea. Caso LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH y Tele2 Telecommunication GmbH. Auto de 19 de febrero de 2009.
- Tribunal de Justicia de la Unión Europea (sala tercera). Caso College van burgemeester en wethouders van Rotterdam vs. M.E.E. Rijkeboer. Sentencia de 7 de mayo de 2009.
- Tribunal de Justicia de la Unión Europea. Caso L'Oreal SA vs eBay. Sentencia de 12 de julio de 2011.
- Tribunal de Justicia de la Unión Europea. Caso Sabam vs. Scarlet. Sentencia de 24 de noviembre de 2011.
- Tribunal de Justicia de la Unión Europea. Casos Volker und Markus Schecke GbR (C-92/09) y Hartmut Eifert (C-93/09) vs. Land Hessen. Sentencia de 9 de noviembre de 2012.
- Tribunal de Justicia de la Unión Europea (sala tercera). Caso Worten – Equipamentos para o Lar, S.A., vs. Autoridade para as Condições de Trabalho. Sentencia de 30 de mayo de 2013

- Tribunal de Justicia de la Unión Europea (sala cuarta). Caso Schwartz vs. Bochum. Sentencia de 17 de octubre de 2013.
- Tribunal de Justicia de la Unión Europea. Caso UPC Telekabel Wien (C- 314/12). Sentencia de 27 de marzo de 2014.
- Tribunal de Justicia de la Unión Europea (Gran Sala). Caso Mario Costeja vs. Google (C-131/12). Sentencia de 13 de mayo de 2014.
- Tribunal de Justicia de la Unión Europea (Sala Séptima). Caso Sotiris Papasavvas vs. O Fileleftheros Dimosia Etaireia. Sentencia de 11 de septiembre de 2014.
- Tribunal de Justicia de la Unión Europea (sala cuarta). Caso Rynes vs. Urad pro ochranu osobnich udaju. Sentencia de 11 de diciembre de 2014.
- Tribunal de Justicia de la Unión Europea (sala tercera). Caso Bara vs. Președintele Casei Naționale de Asigurări de Sănătate. Sentencia de 1 de octubre de 2015.
- Tribunal de Justicia de la Unión Europea (sala tercera). Caso Weltimmo s. r. o. vs. Nemzeti Adatvédelmi és Információszabadság Hatóság. Sentencia de 1 de octubre de 2015
- Tribunal de Justicia de la Unión Europea (Gran Sala). Caso Maximillian Schrems vs. Data Protection Commissioner (C-362/14)). Sentencia de 6 de octubre de 2015.
- Tribunal de Justicia de la Unión Europea (sala segunda). Caso Patrick Breyer vs Germany. Sentencia de 19 de octubre de 2016.
- Tribunal de Justicia de la Unión Europea. Caso Tele2 Sverige AB v Post-ochtelestyrelsen (C-203/15) y Secretary of State for the Home Department vs Tom Watson and Others (C-698/15). Sentencia de 21 de diciembre de 2016.

TEDH

- Tribunal Europeo de Derechos Humanos (Plenario). Caso Tyrer vs. Reino Unido. Sentencia de 25 de abril de 1978.
- Tribunal Europeo de Derechos Humanos (Pleno). Caso Sunday Times vs. Reino Unido. Sentencia de 26 de abril de 1979.
- Tribunal Europeo de Derechos Humanos (Pleno). Caso Lingens vs. Austria. Senencia de 8 de julio de 1986.
- Tribunal Europeo de Derechos Humanos (Pleno). Caso Markt Intern Verlag GmbH and Klaus Beermann vs. Alemania. Sentencia de 20 de noviembre de 1989.
- Tribunal Europeo de Derechos Humanos (Pleno). Caso Burghartz vs Suiza. Sentencia de 22 de febrero de 1994.
- Tribunal Europeo de Derechos Humanos (Gran Sala). Caso Vogt vs Alemania. Sentencia de 26 de septiembre de 1995.
- Tribunal Europeo de Derechos Humanos (Plenario). Caso Z vs. Finlandia. Sentencia de 25 de febrero de 1997.
- Tribunal Europeo de Derechos Humanos. Caso Amann vs. Switzerland. Sentencia de 16 de febrero de 2000

- Tribunal Europeo de Derechos Humanos. Caso Rotaru v Romania. Sentencia de 4 de mayo de 2000.
- Tribunal Europeo de Derechos Humanos. Copland vs. United Kingdom Sentencia de 7 de abril de 2000.
- Tribunal Europeo de Derechos Humanos (Sección tercera). Caso Bensaid vs. Reino Unido. Sentencia de 6 de febrero de 2001.
- Tribunal Europeo de Derechos Humanos (Sección tercera). Caso P.G. y J.H vs. Reino Unido. Sentencia de 25 de septiembre de 2001.
- Tribunal Europeo de Derechos Humanos (Sección segunda). Caso Taylor-Sabori vs. Reino Unido. Sentencia de 22 de octubre de 2002.
- Tribunal Europeo de Derechos Humanos (Sección cuarta). Caso Peck vs. Reino Unido. Sentencia de 28 de enero de 2003.
- Tribunal Europeo de Derechos Humanos (Sección Duodécima). Caso Sociéte Plon vs. France. Sentencia de 18 de mayo de 2004.
- Tribunal Europeo de Derechos Humanos (Sección cuarta). Caso Sciacca vs. Italia. Sentencia de 11 de enero de 2005.
- Tribunal Europeo de Derechos Humanos (sección cuarta). Caso Perrin vs. UK. Sentencia de 18 de octubre de 2005.
- Tribunal Europeo de Derechos Humanos (sección quinta) Caso Panteleyenko vs. Ucrania. Sentencia de 29 de junio de 2006.
- Tribunal Europeo de Derechos Humanos (Primera Sección). Caso Erbakan vs Turkey. Sentencia de 6 de julio de 2006.
- Tribunal Europeo de Derechos Humanos (sección segunda). Caso L.L vs. Francia. Sentencia de 10 de octubre de 2006.
- Tribunal Europeo de Derechos Humanos (Sección Quinta). Caso *Iliya Stefanov vs. Bulgaria* Sentencia de 22 de mayo de 2008.
- Tribunal Europeo de Derechos Humanos (sección segunda) Caso Biriuk vs. Lituania. Sentencia de 25 de octubre de 2008.
- Tribunal Europeo de Derechos Humanos (Gran Sala). Caso Marper vs. Reino Unido. Sentencia de 4 de diciembre de 2008.
- Tribunal Europeo de Derechos Humanos (Sección quinta). Caso Uzun vs. Alemania. Sentencia de 2 de septiembre de 2010.
- Tribunal Europeo de Derechos Humanos (sección quinta). Caso Editorial Board of Pravoye Delo and Shtekel vs. Ukraine. Sentencia de 5 de mayo de 2011.
- Tribunal Europeo de Derechos Humanos (Sección primera). Caso Shimovolos vs. Rusia. Sentencia de 21 de junio de 2011.
- Tribunal Europeo de Derechos Humanos (sección segunda) Caso Godelli vs. Italia. Sentencia de 25 de septiembre de 2012.

- Tribunal Europeo de Derechos Humanos (Sección cuarta). Caso M.M. vs Reino Unido. Sentencia de 13 de noviembre de 2012.
- Tribunal Europeo de Derechos Humanos (sección segunda). Caso Ahmet Yildirim vs Turquía. Sentencia de 18 de diciembre de 2012.
- Tribunal Europeo de Derechos Humanos (Sección quinta). Caso Peruzzo y Martens vs. Alemania. Sentencia de 4 de junio de 2013.
- Tribunal Europeo de Derechos Humanos. Caso bernh Larsen Holding AS and others v Norway App. Sentencia de 8 de julio de 2013.
- Tribunal Europeo de Derechos Humanos (Sección quinta). Caso M.K. vs. Francia. Sentencia de 18 de julio de 2013.
- Tribunal Europeo de Derechos Humanos (sección cuarta). Caso Bartnik v. Poland. Decisión de 11 de marzo de 2014.
- Tribunal Europeo de Derechos Humanos (Sección Cuarta). Caso LH vs Letonia. Sentencia de 29 de abril de 2014.
- Tribunal Europeo de Derechos Humanos (Gran Sala). Caso Mourice vs. France. Sentencia de 23 de abril de 2015.
- Tribunal Europeo de Derechos Humanos (Sección primera). Caso Dragojević vs. Croacia Sentencia de 15 de mayo de 2015.
- Tribunal Europeo de Derechos Humanos (Gran Sala). Caso Delfi vs. Estonia. Sentencia de 16 de junio de 2015.
- Tribunal Europeo de Derechos Humanos (Sección primera). Caso Sõro vs. Estonia. Sentencia de 3 de septiembre de 2015.
- Tribunal Europeo de Derechos Humanos (Sección Primera). Caso Sérvulo & Associados - Sociedade de Advogados, Rl vs. Portugal. Sentencia de 3 de diciembre de 2015.
- Tribunal Europeo de Derechos Humanos. Caso Barbulescu vs. Rumania. Sentencia de 12 de enero de 2016.
- Tribunal Europeo de Derechos Humanos (sección tercera). Caso Vukota-Bojic vs. Switzerland. Sentencia de 18 de octubre de 2016.

TC

- Tribunal Constitucional (Sala Segunda). Sentencia 6/1981, de 16 de marzo.
- Tribunal Constitucional (Sección Tercera). Sentencia 110/1984, de 26 de noviembre.
- Tribunal Constitucional (Sala Segunda). Sentencia 231/1988 de 2 de diciembre.
- Tribunal Constitucional (Sala Primera). Sentencia 20/1990, de 15 de febrero.
- Tribunal Constitucional (Pleno). Sentencia 76/1990, de 26 de abril.
- Tribunal Constitucional. Pleno. Sentencia 160/1991 de 18 de julio.
- Tribunal Constitucional (Sala Segunda). Sentencia 85/1992, de 1 de julio.
- Tribunal Constitucional (Sala Primera). Sentencia núm. 254/1993, de 20 de julio.
- Tribunal Constitucional (Sala Segunda). Sentencia 336/1993, de 15 de noviembre.

- Tribunal Constitucional (Sala Primera). Sentencia 207/1996, de 16 de diciembre.
- Tribunal Constitucional (Sala Segunda). Sentencia 94/1998, de 4 de mayo.
- Tribunal Constitucional (Sala Segunda). Sentencia 44/1999, de 22 de marzo.
- Tribunal Constitucional (Sala Primera). Sentencia 202/1999 de 16 de diciembre.
- Tribunal Constitucional (Sala Primera). Sentencia 98/2000, de 10 de abril.
- Tribunal Constitucional (Sala Primera). Sentencia 186/2000, de 10 de julio.
- Tribunal Constitucional (pleno). Sentencia 290/2000 de 30 de noviembre
- Tribunal Constitucional (Sala Primera). Sentencia 98/2000, de 10 de abril.
- Tribunal Constitucional (Pleno). Sentencia núm. 292/2000 de 30 de noviembre.
- Tribunal Constitucional (Pleno). Sentencia 119/2001, de 24 de mayo.
- Tribunal Constitucional (Sala Segunda). Sentencia 136/2001, de 18 de junio.
- Tribunal Constitucional (Sala Primera). Sentencia 83/2002, de 22 de abril.
- Tribunal Constitucional (Sala Primera). Sentencia 218/2002, de 25 de noviembre.
- Tribunal Constitucional (Sección Tercera). Auto 57/2007, de 26 de febrero.
- Tribunal Constitucional (Sala Segunda). Sentencia 173/2011, de 7 de noviembre.
- Tribunal Constitucional (Sala Primera). Sentencia 142/2012, de 2 de julio.
- Tribunal Constitucional (Sala Primera). Sentencia 241/2012 de 7 de diciembre.
- Tribunal Constitucional (Pleno). Sentencia 17/2013 de 31 de enero
- Tribunal Constitucional (sala primera). Sentencia 29/2013 de 11 de febrero.
- Tribunal Constitucional (Pleno). Sentencia 115/2013, de 9 de mayo.
- Tribunal Constitucional (Sala Primera). Sentencia 170/2013 de 7 de octubre.
- Tribunal Constitucional (Pleno). Sentencia 39/2016, de 3 de marzo.

TS

- Tribunal Supremo (Sección Sexta de la Sala Tercera de lo Contncioso-Administrativo). Sentencia 2778/2007, de 17 de abril de 2007.
- Tribunal Supremo. (Sala de lo Social, Sección 1ª). Sentencia núm. 6128/2007 de 26 de septiembre.
- Tribunal Supremo (Sala de lo Civil). Sentencia 773/2009 de 9 de diciembre.
- Tribunal Supremo (Sala de lo Civil). Sentencia 316/2010, de 18 de mayo.
- Tribunal Supremo (Sala de lo Contencioso-Administrativo, Sección 6ª). Sentencia de 15 de julio de 2010.
- Tribunal Supremo (Sala de lo Civil). Sentencia 72/2011, de 10 de febrero de 2011.
- Tribunal Supremo. (Sala de lo Social, Sección 1ª). Sentencia núm. 1630/2011 de 8 de marzo.
- Tribunal Supremo (Sala de lo Civil). Sentencia 128/2013, de 26 de febrero.
- Tribunal Supremo (Sala Segunda de lo Penal). Sentencia 342/2013, de 17 de abril

AUDIENCIA NACIONAL

- Audiencia Nacional (Sección Primera. Sala de lo Contencioso-Administrativo). Sentencia 6324/2002, de 15 de noviembre de 2002.
- Audiencia Nacional (Sala de lo Contencioso-Administrativo, sección primera). Sentencia de 9 de septiembre de 2004.

AUDIENCIAS PROVINCIALES

- Audiencia Provincial de Madrid. Sentencia de 14 de junio de 2005.
- Audiencia Provincial (Sección 14). Sentencia de 20 de diciembre de 2005.
- Audiencia Provincial de Madrid. Caso Telecinco vs. Youtube. Sentencia de 14 de enero de 2014.
- Corte Suprema. Caso Da Cunha, Virginia c/ Yahoo de Argentina. Sentencia de 30 de diciembre de 2014.

ARGENTINA

- Corte Suprema. Caso Rodríguez vs. Google Inc. Sentencia de 28 de octubre de 2014.

AUSTRALIA

- Tribunal Federal. *Caso Bank of Valletta PLC vs National Crime Authority*. Sentencia de 13 de agosto de 1999.
- Tribunal Supremo del Sur de Australia. Caso Duffy vs. Google. Sentencia de 27 de octubre de 2015.

BRASIL

- Tribunal Superior Federal. Sentencia de 8 de julio de 2009.

CANADÁ

- Tribunal Supremo. Caso R. *v.* Vu. Sentencia de 7 de noviembre de 2013.

COLOMBIA

- Corte Constitucional. Sentencia de 12 de mayo de 2015.
- Corte Constitucional. Sentencia de 10 de febrero de 2016.

COSTA RICA

- Sala Constitucional. Sentencia nº 10627 de 30 de julio de 2009.

ESTADOS UNIDOS

- Tribunal Supremo. Caso Barron vs. Baltimore. Sentencia de 16 de febrero de 1833.

- Corte Suprema de Nueva York. Caso Marion Manola vs. Stevens & Myers. Sentencia de 15 de junio de 1890.
- Tribunal Supremo. Caso Schenk vs. United States. Sentencia de 3 de marzo de 1919.
- Tribunal Supremo. Caso Abrams vs. United States. Sentencia de 10 de noviembre de 1919.
- Tribunal Supremo. Caso Gitlow vs. Nueva York. Sentencia de 8 de junio de 1925.
- Tribunal Supremo. Caso Breard vs. City of Alexandria. Sentencia de 4 de junio de 1951.
- Tribunal Supremo. Cgaso Griswold vs. Connecticut. Sentencia de 7 de junio de 1965.
- Tribunal Supremo. Sentencia Katz vs. United States. Sentencia de 18 de diciembre de 1967.
- Tribunal Supremo. Caso Brandenburg vs Ohio. Sentencia de 8 de junio de 1969.
- Tribunal Supremo. Caso Miller vs. California. Sentencia de 21 de junio de 1973.
- Tribunal de Apelación del Undécimo Circuito. Caso Banco Nova Scotia. Sentencia de 14 de agosto de 1984.
- Tribunal Supremo. Caso City of Ontario vs. Qohn. Sentencia de 31 de marzo de 1987.
- Tribunal Supremo. Caso Hustler Magazine vs. Falwell. Sentencia de 24 de febrero de 1988.
- Tribunal del Distrito Sur de Nueva York. Cubby, Inc. vs. CompuServe Inc, Sentencia de 29 de octubre de 1991.
- Tribunal Supremo. Caso R.A.V. v. City of St. Paul. Sentencia de 22 de junio de 1992.
- Tribunal Supremo de Nueva York. Caso Stratton Oakmont, Inc. v. Prodigy Services Co. Sentencia de 3 de octubre de 1995.
- Tribunal de Distrito Norte de California. Caso Religious Technology Center vs. Netcom On-Line Communication Services, Inc.Sentencia de 21 de noviembre de 1995.
- Tribunal Supremo. Caso ACLU vs. Reno. Sentencia de 26 de junio de 1997.
- Corte de Apelación del Noveno Distrito Federal. Sentencia de 11 de junio de 2001.
- Corte de Apelación del Noveno Circuito. Caso Ashcroft vs. Free Speech Coalition. Sentencia de 16 de abril de 2002.
- Corte de Apelación del Noveno Circuito. Caso Planned Parenthood of the Columbia/Willamette, Inc. v. American Coalition of Life Activists. Sentencia de 16 de mayo de 2002.
- Tribunal Supremo. Caso US vs. American Library Association. Sentencia de 23 de junio de 2003.
- Corte de Apelación del Quinto Distrito del Estado de Florida. Sentencia de 11 de febrero de 2005.
- Tribunal Supremo. Caso Garcetti vs. Ceballos. Sentencia de 30 de mayo de 2006.
- Tribunal del Noveno Circuito Judicial. caso Quon v. Arch Wireless Operating Co. Sentencia de 18 de junio de 2008.
- Tribunal de Apelaciones del Tercer Circuito. Caso ACLU vs. Mukhasey. Sentencia de 22 de julio de 2008.
- Tribunal Supremo de New Jersey. caso Stengart v. Loving Care Agency. Sentencia de 30 de marzo de 2010.
- Tribunal Supremo. caso Stengart v. Loving Care Agency. Sentencia de 19 de abril de 2010.
- Corte de Apelación de California. Gina M Holmes vs. Petrovich Development Company. Sentencia de 13 de enero de 2011.

- Tribunal Supremo. Caso Saskatchewan Human Rights Commission v Whatcott. Sentencia de 27 de febrero de 2013.
- Tribunal Supremo. Caso Ridley vs. California. Sentencia de 25 de junio de 2014.
- Corte de Apelación del Segundo Circuito. Caso Microsoft vs Estados Unidos. Sentencia de 14 de julio de 2016.
- Tribunal de Distrito para el Distrito Este de Pennsylvania. Sentencia de 3 de febrero de 2017.

FRANCIA

- Corte de Casación. Caso Nikon France vs. Onof. Sentencia de 2 de octubre de 2001.
- Consejo Constitucional. N°2009-580. Sentencia de 10 de junio de 2009.
- Corte de Casación. Caso Bruno B v. Giraud et Migot. Sentencia 15 de diciembre de 2009.
- Tribunal de Casación de París. Caso Société Nord-Ouest & UGC Images vs Dailymotion. Sentencia de 17 de febrero de 2011.
- Tribunal de Gran Instancia de París. caso TF1, TF1 Video, TF1 droits audiovisuels, LCI y e-TF1 vs Youtube. Sentencia de 29 de mayo de 2012.
- Corte de Casación. Caso Monsieur X v. Young & Rubicam Franc. Sentencia de 19 de diciembre de 2013.

INDIA

- Tribunal Supremo. Caso Shreya Singhal v. Union of India. Sentencia de 24 de marzo de 2015.

ITALIA

- Tribunal de Distrito de Turín. Sentencia de 20 de agosto de 2006.
- Tribunal de Casación. Sentencia de 19 de diciembre de 2007.
- Tribunal ordinario de Milán (Sección 4ª de lo Penal). Sentencia de 24 de febrero de 2010.
- Tribunal de Apelación de Milán. Caso RETI vs. Yahoo. Sentencia de 7 de enero de 2015.

PAÍSES BAJOS

- Tribunal de Apelación de Leeuwarden de 22 de mayo de 2012. Caso Stokke vs. Marktplaats. Sentencia del 22 de mayo de 2012.

REINO UNIDO

- Alto Tribunal de Justicia. Caso Bunt vs. AOL, Tiscalli y BT. Sentencia de 10 de marzo de 2006.

REPÚBLICA DOMINICANA

- Tribunal Constitucional. Sentencia TC/0484/16 de 18 de octubre de 2016.

VENEZUELA

- Tribunal Supremo de Justicia (Sala Constitucional). Sentencia nº 1053 de 31 de agosto de 2000.
- Tribunal Supremo de Justicia (Sala Constitucional). Sentencia nº 4975 de 15 de diciembre de 2005.
- Tribunal Supremo de Justicia (Sala Constitucional). Sentencia nº 1318 de 4 de agosto de 2011.

AUTORIDADES DE PROTECCIÓN DE DATOS

GRUPO DE TRABAJO DEL ARTÍCULO 29-ARTICLE 29 DATA PROTECTION WORKING PARTY

- Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE. 1998.
- Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo. 2002.
- 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. 30 de mayo de 2002.
- Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). 22 de noviembre de 2006.
- Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda. 4 de abril de 2008.
- Dictamen 5/2009 sobre las redes sociales en línea. 12 de junio de 2009.
- Opinion 1/2010 on the concepts of "controller" and "processor". febrero de 2010.
- Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento".
- Opinion 8/2010 on applicable law. diciembre de 2010.
- Opinion 13/2011 on Geolocation services on smart mobile devices". 16 de mayo de 2011.
- Dictamen 5/2012 sobre la computación en nube. 2012.
- Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules. 6 de junio de 2012.
- Opinion 08/2014 on Personal Data Breach Notification. 25 de marzo de 2014.
- Opinion 8/2014 on the on Recent Developments on the Internet of Things. 16 de septiembre de 2014.
- Working document 01/2014 on Draft Ad hoc contractual clauses "EU data processor to non-EU sub-processor". 2014.
- Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain. 16 de diciembre de 2015.
- Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC). 19 de julio de 2016.

- Guidelines on the right to data portability. 13 de diciembre de 2016.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

- Guía del derecho fundamental a la protección de datos. 2004.
- Informe 582/2004.
- Encargado del tratamiento y obligación de devolución de documentación. Informe 34/2006.
- Informe AEPD 287/2006.
- Informe 0133/2008.
- Informe Jurídico 314/2008.
- Informe 0457/2008.
- Informe 0454/2009.
- Guía de Relaciones Laborales. 2009.
- Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento.
- Dictamen 3/2010, sobre el principio de responsabilidad. 13 de julio de 2010.
- Informe 0227/2010.
- Guía de Seguridad de Datos. 2010.
- Procedimiento 00551/2011.
- Informe 0157/2012.
- Informe 0464/2012.
- Utilización del Cloud Computing por los despachos de abogados y derecho a la protección de datos de carácter personal. 2012.
- Modelo de cláusulas contractuales AEPD para transferencias internacionales de datos entre encargado y subencargado del tratamiento. 21 de marzo de 2012.
- Guía para clientes que contraten servicios de Computing. 2013.
- Informe 0077/2013.
- Expediente TI/00032/2014 Agencia Española de Protección de Datos, “Resolución de declaración de adecuación de garantías para las transferencias internacionales de datos a los Estados Unidos con motivo de la prestación de servicios de computación en nube”, 9 de mayo de 2014.
- Guía para una Evaluación de Impacto en la de Protección Datos Personales. 31 de octubre de 2014.
- Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing., 22 de septiembre 2015.
- Directrices para contratos responsable – encargado. 2017.
- Guía para el cumplimiento del deber de informar. 2017.

- Consultas más frecuentes (FAQS). Garantías a aportar cuando el servicio de Cloud computing implique una transferencia internacional de datos que necesite la autorización de la AEPD.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL)

- Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing. 2012.

DATA PROTECTION COMMISSIONER.

- Data Security Guidance.

DIE DATENSCHUTZBEUFRAGTN ES BUNDES UND DER LÄNDER.

- Orientierungshilfe – Cloud Computing. 9 de octubre de 2014.

FEDERAL DATA PROTECTION INFORMATION COMMISSIONER.

- Guide to cloud computing.

INFORMATION COMMISSIONER (JERSEY) AND DATA PROTECTION COMMISSIONER (GUERNSEY).

- Cloud Computing A guide for data controllers. abril de 2016.

INFORMATION COMMISSIONNER'S OFFICE (ICO)

- Guidance on the use of cloud computing.
- Data controllers and data processors: what the difference is and what the governance implications are. 6 de mayo de 2014.
- Data transfers to the US and Safe Harbor – interim guidance. 10 de febrero de 2016.

WET BESCHERMING PERSOONGEGEVENS.

- Written opinion on the application of the in the case of a contract for cloud computing services from an American provider. 2012.

OTRA DOCUMENTACIÓN

- AENOR. Norma ISO/IEC 27018. Revista AENOR. 20 de noviembre de 2015. Disponible en web: http://www.aenor.es/revista/pdf/nov15/20nov15.pdf
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, INCIBE, CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA. Cómo gestionar una fuga de información en un despacho de abogados.

Octubre 2016. Disponible en web: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/INCIBE_AEPD_Gestionar_fuga_de_informacion.pdf

- AMAZON WEB SERVICES. Whitepaper on EU Data Protection. octubre de 2015. Disponible en web: https://d0.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper_EN.pdf
- ARTHUR COX. Technology Group Briefing. Cloud Computing & The Law. mayo de 2010. Disponible en web: http://www.arthurcox.com/uploadedFiles/Publications/Publication_List/Arthur%20Cox%20-%20Cloud%20Computing%20and%20the%20Law,%20May%202010.pdf
- ASIA CLOUD COMPUTING ASSOCIATION y ASIA PACIFIC CARRIERS COALITION. Report on Cloud Data Regulations. A contribution on how to reduce the compliancy costs of Cross-Border Data Transfers. 2014. Disponible en web: http://trpc.biz/wp-content/uploads/APCC-ACCA_WhitePaper_CloudRegulations_2014_FullPaper.pdf
- BBC. UK surveillance powers explained. November 5th, 2015. Disponible en web: http://www.bbc.com/news/uk-34713435
- BERKMAN CENTER FOR INTERNET AND SOCIETY, *Introduction, Privacy in the Workplace* [en línea]. Disponible en web: https://cyber.harvard.edu/privacy/Module3_Intronew.html#_ftn1
- BIRD&BIRD. Cloud computing and privacy series: security requirements and guidance. 1 de diciembre de 2014. Disponible en web: http://www.twobirds.com/en/news/articles/2014/global/cloud-computing-series-security-requirements-and-guidance
- BLANCO CERTIFIED DATA ERASURE. Soluciones de borrado de datos para centro de datos y seguridad de computación en nube. Blanco White Paper. 2ª edición. 26 de noviembre de 2013. Disponible en web: https://www.ontrackdatarecovery.es/CMS/PDF/white-paper-data-centre-es.pdf
- BUSINESS SOFTWARE ALLIANCE. Cloud Computing Policy Agenda for Europe. Disponible en web: http://www.bsa.org/country/~/media/files/policy/engb/bsaeucloudagenda.ashx
- C-SIG SUB-GROUP ON THE DATA PROTECTION CODE OF CONDUCT. Data Protection. Code of Conduct for Cloud Service Providers. Disponible en web: https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-code-conduct
- CENTER FOR ECONOMICS AND BUSINESS RESEARCH. THE CLOUD DIVIDEND: Part One *The economic benefits of cloud computing to business and the wider EMEA economy France, Germany, Italy, Spain and the UK*. December 2010. Disponible en web: https://uk.emc.com/collateral/microsites/2010/cloud-dividend/cloud-dividend-report.pdf
- CLOUD COMPUTING USE CASE DISCUSSION GROUP. Cloud compunting Use Cases White Paper. Version 4.0. 2 de julio de 2010. Disponible en web: http://open*cloud*manifesto.org/*Cloud*_Computing_Use_Cases_Whitepaper-4_0.pdf

- CLOUD SECURITY ALLIANCE. Guia para la Seguridad en áreas críticas de atención en *Cloud computing*. noviembre de 2009. Disponible en web: http://www.ismsforum.es/img/a25/na235_GUIA_CSA_PARA_LA_SEGURIDAD_EN_AREAS_CRITICAS_DE_ATENCION_EN_*CLOUD*_COMPUTING_V2.pdf
- CLOUD SECURITY ALLIANCE. GRUPO DE TRABAJO-PRIVACY LEVEL AGREEMENT. Esquema de Privacy Level Agreement (PLA) para la Venta de Servicios en la Nube en la Unión Europea, julio de 2013. Disponible en web: https://www.ismsforum.es/ficheros/descargas/acuerdo-de-nivel-de-privacidad1374159133.pdf
- CLOUD SECURITY ALLIANCE. Security Guidance for Critical Areas in Cloud Computing. V3.0 2011. Disponible en web: https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf
- CLOUD SECURITY ALLIANCE. SPANISH CHAPTER. Cloud Compliance Report. 1 de mayo de 2011. Disponible en web: http://clubgertech.unavarra.es/getfile.php?file=Jornadas/11CloudComputing/des144_Cloud_Compliance_Report_CSA-ES_V.1.0.pdf
- CLOUD SELECT INDUSTRY GROUP (C-SIG). Data Protection Code of Conduct for Cloud Service Providers. Disponible en web: https://ec.europa.eu/digital-agenda/en/news/data-protection-code-conduct-cloud-service-providers
- CLOUD SELECT INDUSTRY GROUP–SUBGROUP ON SERVICE LEVEL AGREEMENT (C-SIG-SLA). Cloud Service Level Agreement Standardisation Guidelines. 26 de junio de 2014. Disponible en web: https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines
- CLOUD STANDARDS CONSUMER COUNCIL. Interoperability and Portability for Cloud Computing: A Guide", noviembre de 2014. Disponible en web: http://www.cloud-council.org/deliverables/CSCC-Interoperability-and-Portability-for-Cloud-Computing-A-Guide.pdf
- CLOUDWATCHHUB. The CloudWATCH Legal Guide to the Cloud for SMEs. Disponible en web: http://www.cloudwatchhub.eu/sites/default/files/CloudWATCH_Legal-guide-to-the-cloud.pdf
- COCO CLOUD (CONFIDENCIALITY AND COMPLIANCE IN THE CLOUD). First Study of Legal and Regulatory Aspects of Cloud Computing. Version 1.0. 31 de octubre de 2014. 236 p. Disponible en web: http://www.coco-cloud.eu/sites/default/files/cococloud/files/content-files/deliverables/Coco_Deliverable%20D2.2_UO_20141031(1of2).pdf
- COMISIÓN EUROPEA. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. La protección de la privacidad en un mundo interconectado Un marco europeo de protección de datos para el siglo XXI. COM (2012) 9 final. Disponible en web: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:ES:PD

- COMISIÓN EUROPEA. Decisión de la Comisión de 5 de febrero de 2010 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. 2010. Disponible en web: https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/decisiones/common/pdfs/decision_comm_clausulas_contractuales_2010.pdf
- COMISIÓN EUROPEA. 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. Disponible en web: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52012DC0529&from=ES
- COMISIÓN EUROPEA. Comunicado de Prensa. La Comisión propone una reforma general de las normas de protección de datos para aumentar el control de los usuarios sobre sus propios datos y reducir los costes para las empresas. 25 de enero de 2012. Disponible en web: http://europa.eu/rapid/press-release_IP-12-46_es.htm
- COMISIÓN EUROPEA. Guía acerca del Escudo de Privacidad UE-EE.UU. 2016. Disponible en web: https://www.agpd.es/portalwebAGPD/noticias-inicio/common/pdf/2016/08_agosto/es_56972_citizens-guide_en.pdf
- COMISIÓN EUROPEA. Nota de Prensa de 2 de febrero de 2016, "La Comisión Europea y los Estados Unidos acuerdan un nuevo marco para los flujos transatlánticos de datos: Escudo de la privacidad UE - EE.UU", http://europa.eu/rapid/press-release_IP-16-216_es.htm
- CONSEJO DE EUROPA. Asamblea parlamentaria. Resolución 509 de 31 de enero de 1968 sobre Los derechos humanos y los nuevos logros científicos y técnicos. Disponible en web: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=14546&lang=en
- CONSEJO DE EUROPA. Comité de Ministros. Resolución 22 de 26 de septiembre de 1973 sobre protección de la privacidad de los individuos vis a vis los bancos de datos electrónicos en el sector privado. Disponible en web: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000001680502830
- CONSEJO DE EUROPA. Comité de Ministros. Resolución 29 de 20 de septiembre de 1974 sobre protección de la privacidad de los individuos vis a vis los bancos de datos electrónicos en el sector público. Disponible en web: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d1c51
- CONSEJO DE EUROPA. European Court of Human Rights. Factsheet – Personal data protection. November 2016. Disponible en web: http://www.echr.coe.int/Documents/FS_Data_ENG.pdf
- CONSEJO DE EUROPA. TRIBUNAL EUROPEO DE DERECHOS HUMANOS. AGENCIA EUROPEA DE DERECHOS FUNDAMENTALES. *Handbook on European data protection law*.

2014. Disponible en Web: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf.

- CONSEJO FISCAL. Informe al Anteproyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas. Disponible en web: http://pdfs.wke.es/2/2/7/8/pd0000102278.pdf
- CORTE INTERAMERICANA DE DERECHOS HUMANOS. Relatoria Especial para la Libertad de Expresión. *El derecho de acceso a la información en el marco jurídico interamericano*. 2010. Disponible en web: http://www.oas.org/es/cidh/expresion/docs/publicaciones/ACCESO%20A%20LA%20INFORMACION%20FINAL%20CON%20PORTADA.pdf
- COUNCIL OF EUROPE. Internet: case-law of the European Court of Human Rights, 2015. Disponible en web: http://www.echr.coe.int/documents/research_report_internet_eng.pdf
- COUNCIL OF EUROPE. Assembly. Resolution 1987 (2014). 9 de abril de 2014. Disponible en Web: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=20870&lang=en
- COUNCIL OF EUROPE. T-CY Cloud Evidence Group. Criminal justice access to data in the cloud: challenges. 26 de mayo de 2015. Disponible en web: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2015/T-CY(2015)10_CEG%20challenges%20rep_sum_v8.pdf
- DATA PRIVACY INSTITUTE-ISMS FORUM SPAIN. Estudio de impacto y comparativa con la normativa española de la propuesta de Reglamento General de Protección de Datos de la Unión Europea. 2016. Disponible en web: https://www.ismsforum.es/ficheros/descargas/estudio-reglamento-ue-dpi1353525776.pdf
- DER KONFERENZ DERE DATENSCHUTZBEAUFTRAGTEN DES BUNDES UND DER LÄNDER SOWIE DER ARBEITSGRUPPE INTERNATIONALER DATENVEKEHR DES DÜSSELDORFER KREISSES. Orientierungshilfe – Cloud Computing. 9 de octubre de 2014. Disponible en web: https://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf
- DIGITAL EUROPE. Law Enforcement Access to Data in the European Cloud. Disponible en web: http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=849&language=en-US&PortalId=0&TabId=353
- DIGITALISERINGSSTLYRELSEN. Cloud computing and the legal framework- Guidance on legislative requirement and the contractual environment related to cloud computing. 27 de agosto de 2012. Disponible en web: http://digitaliser.dk/resource/2368677
- ECONOMIC AND SOCIAL COMMITTEE OF THE EUROPEAN UNION. Cloud computing revolution - Why and how should Europe get ready? Disponible en web: http://www.eesc.europa.eu/?i=portal.en.ten-opinions.20566

- ENISA. Cloud computing: Benefits, risks and recommendations for information security. Noviembre 2009. 125 p. Disponible en web: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/
- ENISA. Computación en nube. Beneficios, riesgos y recomendaciones para la seguridad de la información. 2009.
- EUROPE PRIVACY SEALS. Cloud Computing and European Data Protection Law. 2012.
- EUROCLOUD AUSTRIA. Cloud contracts. What providers and consumers should discuss. Version 1.0. 1 November 2012. Disponible en web: http://www.cloudingsmes.eu/wordpress/wp-content/uploads/2014/07/CLOUD_Contracts_EN1.pdf
- EUROCLOUD DEUTSCHLAND. Guidelines Cloud Computing German Law, Data Protection & Compliance. 2014. Disponible en web: http://www.cloudingsmes.eu/wordpress/wp-content/uploads/2014/07/EuroCloud_GuidelineLaw-DP-C_EN1.pdf
- EUROPEAN COMMISSION, Why do we need an EU Data Protection Reform? Disponible en web: http://ec.europa.eu/justice/data-protection/index_en.htmç
- EUROPEAN COMMISSION, European Cloud Computing Strategy, https://ec.europa.eu/digital-single-market/en/european-cloud-computing-strategy
- EUROPEAN COMMISSION. Expert Group Report, The Future of Cloud computing. Opportunities for European Cloud computing Beyond 2010. 2010. 66 p. Disponible en web: http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf
- EUROPEAN COMMISSION. 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. 25 de mayo de 2012. Disponible en web: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf
- EUROPEAN COMMISSION. Directorate-General for Internal Policies. Fighting cyber crime and protecting privacy in the cloud. 2012. Disponible en web: http://www.ptools.com/Blog/Fighting-Cyber-Crime-and-Protecting-Privacy-in-the-Cloud.pdf
- EUROPEAN COMMISSION. Code of EU online rights. Diciembre de 2012. Disponible en web: https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/Code%20EU%20online%20rights%20EN%20final%202.pdf
- EUROPEAN COMMISSION. DECISION of 18 June 2013 on setting up the Commission expert group on cloud computing contracts. Disponible en web: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:174:0006:0008:EN:PDF

- EUROPEAN COMMISSION. Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EUU.S. Data Flows, COM (2013) 846 final, 27 de noviembre de 2013. Disponible en web: http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf
- EUROPEAN COMMISSION. Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies established in the EU, COM(2013) 847 final, 27 de noviembre de 2013 Disponible en web: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf
- EUROPEAN COMMISSION. Case No COMP/M.7217 - FACEBOOK/ WHATSAPP. 3 de octubre de 2014. Disponible en web: http://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf
- EUROPEAN COMMISSION. Code of conduct on countering ilegal hate speech online. 2016. Disponible en web: http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf
- EUROPEAN COMMISSION. Synopsis report on the contributions to the public consultation on the regulatory environment for data and cloud computing. 12 de mayo de 2016. Disponible en web: https://ec.europa.eu/digital-single-market/en/news/synopsis-report-contributions-public-consultation-regulatory-environment-data-and-cloud
- EUROPEAN COMMISSION. Commission implementing decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield. COM (2016) 4176 final, 12 de julio de 2016. Disponible en web: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf
- EUROPEAN COMMITTEE FOR INTEROPERABLE SYSTEMS. Cloud Switching and the free flow of data – portability and interoperability of software and data across cloud services. 27 de junio de 2016. Disponible en web: http://www.ecis.eu/2016/06/special-paper-on-cloud-computing-portability-and-interoperability/
- EUROPEAN DATA PROTECTION SUPERVISOR. Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe". 2012. Disponible en web: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf
- EUROPEAN TELECOMMUNICATIONS STANDARD INSTITUTE. Cloud; SLAs for Cloud Services. Technical Report. 2012. Disponible en web: https://www.etsi.org/deliver/etsi_tr/103100_103199/103125/01.01.01_60/tr_103125v010101p.pdf
- EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. Cloud Standards Coordination Final Report. noviembre de 2013. Disponible en web: http://www.etsi.org/images/files/events/2013/2013_csc_delivery_Ws/csc-Final_report-013-csc_Final_report_v1_0_pdF_format-.pdF

- EXPERT GROUP MEETING ON CLOUD COMPUTING CONTRACTS. Synthesis of the meeting of 29/30 January 2014. Disponible en web: http://ec.europa.eu/justice/contract/files/expert_groups/29_30_jan_meeting_final_synthesis_en.pdf
- FINANCIAL TIMES. Cloud computing hinders data deletion. 18 de marzo de 2013. Disponible en web: https://www.ft.com/content/0e8aad72-7444-11e2-80a7-00144feabdc0
- FUNDACIÓN DE LA INNOVACIÓN BANKINTER y ACCENTURE. Cloud computing. La tercera ola de las Tecnologías de la Información. 2010. p. 22, http://www.fundacionbankinter.org/system/documents/8156/original/XIII_FTF_CloudComputing.pdf
- IBM INSTITUTE FOR BUSINESS VALUE. The power of cloud. Driving business model innovation. Febrero 2012. Disponible en web: http://public.dhe.ibm.com/common/ssi/ecm/en/gbe03471usen/GBE03471USEN.PDF
- IBM. Review and summary of cloud service level agreements - From Cloud Computing Use Cases Whitepaper Versión 4.0. Disponible en web: http://public.dhe.ibm.com/software/dw/cloud/library/cl-rev2sla-pdf.pdf
- INSTITUTO DE CIBERSEGURIDAD (INCIBE). La ciberseguridad a un clic de tu empresa. Disponible en web: https://www.incibe.es/empresas/que_te_interesa/Contratacion_de_servicios/
- INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS. Estudio sobre recomendaciones generales para la destrucción segura de datos personales en ambiente físico y electrónico. diciembre de 2014.
- INTECO (actual INCIBE). Riesgos y amenazas en Cloud Computing. Ministerio de Industria, Turismo y Comercio. marzo de 2011. Disponible en web: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf
- INTERNATIONAL DATA CORPORATION. Worldwide Semiannual Public Cloud Services Spending Guide. 2016.
- INTERNATIONAL LABOUR ORGANIZATION. Protection of workers' personal data. 1997. Disponible en web: http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf
- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 17788. Information technology -- Cloud computing -- Overview and vocabulary
- INTERNATIONAL TELECOMMUNICATIONS UNIT. Privacy in Cloud Computing. marzo de 2012. Disponible en web: https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf
- INTERNET RIGHTS AND PRINCIPLES DYNAMIC COALITION. Carta de Derechos Humanos y Principios en Internet. Disponible en Web: http://diadeinternet.org/pdfs/Internet_Derechos_Principios.pdf

- IT LAW GROUP. USA Patriot Act Effect on Cloud Computing Services. Disponible en web: http://www.itlawgroup.com/resources/articles/113-usa-patriot-act-effect-on-cloud-computing-services
- INTERNET SOCIETY. Brief History of the Internet. Disponible en web: http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet
- ITU-T. Technology Watch Report. Privacy in Cloud Computing. marzo de 2012. Disponible en web: https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf
- KPMG, Modeling the economic impact of *cloud computing* [en línea], May, 2012. http://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Documents/modelling-economic-impact-*cloud*-computing.pdf
- KROMMAN REUMERT. Government Access to Information in the Cloud. marzo de 2012.
- LINKLATERS. Law Enforcement and Cloud Computing. octubre de 2011. Disponible en web: http://www.linklaters.com/Insights/law-enforcement-cloud-computing/Pages/Index.aspx
- MAYER BROWN. Cloud Computing May Violate German Data Privacy Laws. 20 de julio de 2010. Disponible en web: http://www.mayerbrown.com/files/Publication/aef6b505-6895-43b2-9bf8-6d1423e5a61d/Presentation/PublicationAttachment/b31735d9-fc20-4e67-a5db-79d6cd77f659/WORD_Cloud-Computing_0710_V1.pdf
- MICROSOFT. A guide to Data Governance for Privacy, Confidentiality, and Regulatory Compliance. Part 5: Moving to cloud computing. agosto de 2010, Disponible en web: http://www.microsoft.com/privacy/datagovernance.aspx
- MICROSOFT. Recomendaciones sobre la política El acceso gubernamental a los datos. Disponible en web: https://news.microsoft.com/cloudforgood/_media/downloads/es/government-access-to-data-es.pdf
- MLEX. Cloud computing: obligations under the Directive v. GDPR. Junio de 2016. Disponible en web: http://www.mmlex.it/wp-content/uploads/2016/09/DPLP-June-2016-Cloud-Computing.pdf
- NACIONES UNIDAS. Directrices para la regulación de los archivos de datos personales informatizados. 14 de diciembre de1990. Disponible en web: http://inicio.ifai.org.mx/Estudios/D.3BIS-cp--Directrices-de-Protecci-oo-n-de-Datos-de-la-ONU.pdf
- NEXA CENTER FOR INTERNET&SOCIETY. Declaración de los derechos en Internet. Disponible en web: https://nexa.polito.it/nexacenterfiles/dichiarazione-diritti-internet-spagnolo.pdf
- NIST CLOUD COMPUTING REFERENCE ARCHITECTURE AND TAXONOMY WORKING GROUP. Cloud Computing Service Metrics Description. Disponible en web: http://www.nist.gov/itl/cloud/upload/RATAX-CloudServiceMetricsDescription-DRAFT-20141111.pdf
- PINSENT MASONS. Google's cloud database management service offers EU-only data storage and processing. Disponible en web:, http://www.out-law.com/en/articles/2012/november/googles-cloud-database-management-service-offers-eu-only-data-storage-and-processing/

- QUEEN MARY COLLEGE. UNIVERSITIY OF LONDON. Cloud Legal Project. Materiales disponibles en web: http://www.cloudlegal.ccls.qmul.ac.uk/
- OBSERVATORIO NACIONAL DE LAS TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN (ONTSI). Cloud computing. Retos y Oportunidades. Ministerio de Industria, Energía y Turismo. mayo 2012. Disponible en web: http://www.ontsi.red.es/ontsi/sites/default/files/1-_estudio_cloud_computing_retos_y_oportunidades_vdef.pdf
- OBSERVATORIO SAGE. Radiografía SAGE de la PYME en España 2015.
- OECD. Cloud Computing: The Concept, Impacts and the Role of Government Policy. *OECD Digital Economy Papers*. 2014. nº. 240, Paris. Disponible en web: http://dx.doi.org/10.1787/5jxzf4lcc7f5-en
- OPEN CLOUD MANIFESTO. A call to action for the worldwide cloud community. 2009. Disponible en web: https://gevaperry.typepad.com/Open%20Cloud%20Manifesto%20v1.0.9.pdf
- ORACLE. Data Processing Agreement for Oracle Cloud Services. Versión de 31 de julio de 2015. Disponible en web: http://www.oracle.com/us/corporate/contracts/cloud-dpa-2625278.pdf.
- ORGANIZACIÓN DE ESTADOS AMERICANOS. Declaración Conjunta sobre Libertad de Expresión e Internet, 2011.
- PARLAMENTO EUROPEO. Resolución del Parlamento Europeo, de 10 de diciembre de 2013, sobre la liberación del potencial de la computación en la nube en Europa. 10 de diciembre de 2013. Disponible en web: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0535+0+DOC+XML+V0//ES
- REEDSMITH. Transcending the Cloud: A Legal Guide to the Risks and Rewards of Cloud Computing. Cloud Computing-A German Perspective. Disponible en web: https://www.reedsmith.com/files/Publication/cf6df614-498c-4c92-979c-454346c15369/Presentation/PublicationAttachment/131ec3c6-65ff-45e4-bca1-f5628e478465/Cloud%20Computing%20-%20Germany%20Chapter%20ONLY%20-%2008.12.10.pdf
- SEARCHCLOUDCOMPUTING.COM. E-guide. Differences explained: Private vs. public vs. hybrid cloud computing. Sponsored by HP and Intel. Disponible en web: http://docs.media.bitpipe.com/io_10x/io_100433/item_419065/HPIntel_sCloudComputing_SO%23034437_E-Guide_052611.pdf
- SENADO. Comisión Especial de Redes Informáticas. Informe Final. Boletín Oficial de las Cortes Generales, Senado, Serie I, nº 812, 27 de diciembre de 1999.
- SLALOM. Model Contract for Cloud Computing. 21 de marzo de 2016. Disponible en web: http://slalom-project.eu/sites/slalom/files/content-files/article/SLALOM%20Legal%20model_clauses%20only_v1.2.pdf

- TECH UK. TechUK Cloud 2020 Vision. Keeping the UK at the forefront of cloud adoption", marzo de 2016.
- TIME.LEX CVBA y SPARK LTD. Standards terms and performance criteria in service level agreements for cloud computing services. 2015. Disponible en web: http://www.sla-ready.eu/sites/default/files/Finalreport.pdf
- UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. Privacy in the Cloud Computing. Mayo de 2012. Disponible en web: http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf
- UNIÓN EUROPEA. Comunicación de la Comisión Europea sobre la Estrategia de un Mercado Único Digital para Europa, COM (2015) 192 final, Bruselas, 6 de mayo de 2015. Disponible en web: http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf
- UNITED NATIONS. Human Rights Council. The promotion, protection and enjoyment of human rights on the Internet. 12 de julio de 2016. Disponible en Web: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf
- US DEPARTMENT OF COMMERCE'S INTERNATIONAL TRADE ADMINISTRATION (ITA) Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing. Disponible en web: https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2013/04/Safe-Harbor-and-Cloud-Computing-Clarification_April-12-2013_Latest_eg_main_060351.pdf
- US ENVIRONMENTAL PROTECTION AGENCY. ENERGY STAR PROGRAM. Report to Congress on Server and Data Center Energy Efficiency. Public Law 109-431. August 2, 2007. Disponible en web: https://www.energystar.gov/sites/default/files/buildings/tools/Report%20to%20Congress%20on%20Server%20and%20Data%20Center%20Energy%20Efficiency.pdf
- WORLD ECONOMIC FORUM IN PARTNERSHIP WITH ACCENTURE. Advancing Cloud Computing: What to Do Now? 2011. Disponible en web: http://www3.weforum.org/docs/WEF_IT_AdvancedCloudComputing_Report_2011.pdf
- WORLD ECONOMIC FORUM, *The Future of Jobs Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution*, January 2016. Disponible en web: http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf

ANEXO I

ABREVIATURAS MÁS FRECUENTES

AGPD: Agencia Española de Protección de Datos
CDFUE: Carta de Derechos Fundamentales de la Unión Europea
CE: Constitución Española
LECrim: Ley de Enjuiciamiento Criminal
LOPD: Ley Orgánica de Protección de Datos
LORTAD: Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de carácter personal
PSI: Prestadores de Servicios de Intermediación
RGPD: Reglamento General de Protección de Datos
ROPD: Reglamento Orgánico de Protección de Datos
TC: Tribunal Constitucional
TJUE: Tribunal de Justicia de la Unión Europea
TEDH: Tribunal Europeo de Derechos Humanos
TS: Tribunal Supremo
STC: Sentencia del Tribunal Constitucional
STEDH: Sentencia del Tribunal Europeo de Derechos Humanos
STJUE: Sentencia del Tribunal de Justicia de la Unión Europea
STS: Sentencia del Tribunal Supremo