TESIS DOCTORAL

«EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO DE LA PREVENCIÓN Y REPRESIÓN PENAL EUROPEA
(En busca del equilibrio entre la libertad y la seguridad)»

Tesis para optar al grado de Doctor en Derecho Público del
Programa: *"Las Transformaciones del Estado de Derecho desde la perspectiva de la Filosofía del Derecho, el Derecho Constitucional y el Derecho Penal*"

Autor: Alejandro Luis Gacitúa Espósito

Director: Dr. Joan Lluís Pérez Francesch

Departamento de Ciencia Política y de Derecho Público

Universidad Autónoma de Barcelona

Barcelona, Mayo de 2014

TESIS DOCTORAL

«EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO DE LA PREVENCIÓN Y REPRESIÓN PENAL EUROPEA (En busca del equilibrio entre la libertad y la seguridad)»

Director: Dr. Joan Lluís Pérez Francesch

Doctorando: Sr. Alejandro Luis Gacitúa Espósito

A mi hija Amalia

“La libertad no es nada más que una oportunidad para ser mejor”.

- Albert Camus

“El hombre ha nacido libre, pero por todas partes se encuentra rodeado de cadenas”.

- Jean-Jacques Rousseau

ÍNDICE

CAPÍTULO TERCERO

DIRECTRICES INTERNACIONALES SOBRE PROTECCIÓN DE DATOS PERSONALES

SEGUNDA PARTE

MARCO NORMATIVO DE LA PROTECCIÓN DE DATOS CON FINES DE PREVENCIÓN Y REPRESIÓN PENAL EN LA COOPERACIÓN POLICIAL EUROPEA

CAPITULO CUARTO

NORMATIVA DEL CONSEJO DE EUROPA Y SU IMPORTANCIA PARA LA MATERIA EN ESTUDIO

CAPÍTULO QUINTO

NORMATIVA GENERAL DE LA UNIÓN EUROPEA EN MATERIA DE PROTECCIÓN DE DATOS

CAPÍTULO SEXTO

MARCO JURÍDICO DE LA PROTECCIÓN DE DATOS EN EL ÁMBITO ESPECÍFICO DE LA COOPERACIÓN POLICIAL O CON INCIDENCIA EN ÉL

TERCERA PARTE

TRATAMIENTO DE LOS DATOS PERSONALES EN EL ÁMBITO DE LA PREVENCIÓN Y REPRESIÓN PENAL EUROPEA

CAPÍTULO SEPTIMO

ANALISIS CRÍTICO DE ALGUNOS ASPECTOS SUBJETIVOS DEL TRATAMIENTO DE DATOS CON FINES DE PREVENCIÓN Y REPRESIÓN PENAL

CAPITULO OCTAVO

TRANSFERENCIA DE DATOS PERSONALES A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES

AGRADECIMIENTOS

Esta tesis ha sido fruto de una decisión personal, pero ella no habría visto la luz, sin el apoyo de personas e instituciones que hicieron posible su realización a través del apoyo emocional, económico o académico.

En primer lugar quiero agradecer a mi mujer, Su, por haberme acompañado en esta etapa de mi vida y por haber confiado en mí y apoyado en los momentos más difíciles. También, a ti mi pequeña Amalia, que has nacido durante este proceso y me has dado las fuerzas necesarias para llegar a puerto. A mis padres, Marianela y Alejandro, y mis hermanos César y Rodrigo, por el cariño y apoyo incondicional, incluso a la distancia.

También quisiera agradecer, al Programa Capital Humano Avanzado, de la Comisión Nacional de Investigación Científica y Tecnológica (CONICYT) del Gobierno de Chile, por haberme otorgado la Beca Presidente de la República, que permitió financiar la realización de mis estudios de Doctorado en la Universidad Autónoma de Barcelona.

Además, quisiera agradecer a mis profesores y compañeros del Doctorado en Derecho Público de la Facultad de Derecho de la Universidad Autónoma de Barcelona, y particularmente a Tomas Gil y Josep Cañabate, así como también a mis colegas de la Facultad de Derecho de la Universidad Central de Chile, por el apoyo, la comprensión y buena disposición en el proceso final de mi tesis.

Por último, quiero agradecer muy especialmente a mi director de la Tesis Doctoral el profesor Dr. Joan Lluís Pérez Francesch por el apoyo, la paciencia y la generosidad en la entrega de sus conocimientos. Sin lugar a dudas el haber trabajo con él durante este tiempo me ha marca en lo personal, ya que me ha demostrado, a través de su ejemplo, que se puede hacer investigación y docencia con humildad y excelencia.

ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
APEC	Foro de Cooperación Económica Asia Pacífico
APD	Autoridades de Protección de Datos
APDCAT	Agencia Catalana de Protección de Datos
APD	*Advance Passenger Information*
BOE	Boletín Oficial del Estado
CBP	*Bureau of Customs and Border Protection*
CBPR	*Crossborder Privacy Rules*
CBSA	*Canada Border Services Agency*
CDFUE	Carta de Derechos Fundamentales de la Unión Europea
CE	Constitución Española de 27 de diciembre de 1978
CEDH	Convenio Europeo de Derechos Humanos
CEPOL	Escuela Europea de Policía
CJCE	Corte de Justicia de las Comunidades Europeas
CPEA	*Cross-Border Privacy Enforcement Arrangement*
DHS	*Department of Homeland Security*
DM	Decisión Marco
DOCE	Diario Oficial de las Comunidades Europeas
DOUE	Diario Oficial de la Unión Europea
DUDH	Declaración Universal de Derechos Humanos
EIPD	Encuentro Iberoamericano de Protección de Datos
EURODAC	Sistema Europeo de Comparación de Huellas Dactilares
EUROJUST	Unidad de Cooperación Judicial Europea
EUROPOL	Oficina Europea de Cooperación Policial
EUROSIGMA	Agencia Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia
FRONTEX	Agencia Europea para la gestión de la cooperación operativa en las fronteras exteriores de los Estados miembros de la Unión
GT29	Grupo de protección de las personas en lo que respecta al tratamiento de datos personales (art. 29 de La Directiva 95/46).

LOPD	Ley Orgánica 15/1999, de 13 de diciembre. Protección de Datos de Carácter Personal
LORTAD	Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal
OCDE	Organización para la Cooperación y el Desarrollo Económico
OIG	Organizaciones Internacionales Gubernamentales
OLAF	Oficina Europea de Lucha contra el Fraude
ONU	Organización de las Naciones Unidas
OSI	*Other Service Information*
PAD	Procesamiento automático de datos
PIDCP	Pacto Internacional de Derechos Civiles y Políticos
RDAEPD	Real Decreto por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos
RDLOPD	Reglamento de desarrollo de la Ley Orgánica de Protección de Datos personales
RIPD	Red Iberoamericana de Protección de Datos
SEPD	Supervisor Europeo de Protección de Datos
SAA	Servicios de Aduanas de Australia
SIA	Sistema de Información Aduanera
SIS	Sistema de Información Schengen
SIR	Sistema de Informatizados de Reserva
SIV	Sistema de Información de Visados
SSI	*Special Services Information*
SSR	*Special Services Reserved*
TCE	Tribunal Constitucional Español
TCFA	Tribunal Constitucional Federal Alemán
TCCE	Tratado Constitutivo de la Comunidad Europea
TEDH	Tribunal Europeo de Derechos Humanos
TFUE	Tratado de Funcionamiento de la Unión Europea
TIC	Tecnologías de la información y la comunicación
TID	Transferencia internacional de datos
TJCE	Tribunal de Justicia de la Comunidades Europeas
TJUE	Tribunal de Justicia de la Unión Europea
TUE	Tratado de la Unión Europea

UE	Unión Europea
UIP	Unidades de Información sobre Pasajeros

INTRODUCCIÓN

SUMARIO: 1. Presentación; 2. Planteamiento del problema; 3. Objeto de la investigación; 4. Enfoque metodológico; 5. Contenido de la investigación.

1. Presentación

La presente tesis doctoral fue realizada dentro del programa de Doctorado que imparte el Departamento de Ciencia Política y Derecho Público de la Universidad Autónoma de Barcelona, denominado: "Las Transformaciones del Estado de Derecho desde la perspectiva de la Filosofía del Derecho, el Derecho Constitucional y el Derecho Penal". Su objeto es el análisis del derecho fundamental a la protección de datos personales en el ámbito de la cooperación policial europea en materias penales, y se enmarca dentro de la línea de trabajo que realiza el "Grupo de estudio sobre libertad, seguridad y transformaciones del Estado", que dirige el Dr. Joan Lluís Pérez Francesch, en la misma Universidad.

El desarrollo de este trabajo ha tenido lugar en dos etapas. La primera, corresponde al periodo comprendido entre el 2010 y el 2011, y en el realizamos la recopilación y análisis preliminar del material doctrinario, legislativo y jurisprudencial para dar inicio al trabajo, elaboramos el proyecto de investigación e inscribimos la presente tesis doctoral bajo la dirección del profesor Dr. Joan Lluís Pérez Francesch. La segunda parte, ha tenido lugar en el periodo 2012 y 2013, desde Chile, periodo en el cual fue redactada la tesis. Por último, durante enero y febrero de 2014, se han realizado las correcciones y actualizaciones necesarias para terminar el presente trabajo y ser depositada para su posterior lectura y defensa ante los miembros del tribunal.

A primera vista, puede parecer extraño que un abogado y académico chileno se interese en investigar el tema que se plantea en esta tesis, la cual versa sobre una temática, en apariencia, exclusivamente Europea. No obstante, estamos convencidos de que fue una decisión acertada, ya que el derecho en la actualidad tiene implicaciones cada vez más globales, y la temática elegida no escapa a ello. Además, el bagaje y la

experiencia europea siempre ha sido considerada en Latinoamérica y en Chile en particular en el proceso de adopción de normas jurídicas, lo que ha permitido que los principios esenciales que guían el derecho europeo continental crucen el atlántico y sirvan de inspiración en el continuo proceso de la revisión y reelaboración del derecho. Por último, también influyó en la decisión del tema el hecho de haber cursado un Master en Auditoria y Protección de Datos Personales, que impartió la Universidad Autónoma de Barcelona en conjunto con la Agencia Catalana de Protección de Datos, lo que me brindó una primera aproximación conceptual y teórica al mundo de los datos personales.

2. Planteamiento del problema

Si bien la utilización de medios técnicos para realizar labores de control y fiscalización por parte de los organismos encargados de la seguridad pública no es un hecho nuevo en la historia de la humanidad, lo que es diferente hoy son los alcances y facilidades que ofrecen los adelantos tecnológicos para dicha actividad. La tecnología actual permite no sólo evaluar la información que directa o indirectamente facilitan las personas, sino que también ha llegado al punto de permitir elaborar perfiles de personalidad y predicciones de comportamientos, todo gracias a la enorme velocidad y capacidad para procesar grandes volúmenes de datos. Ello ha facilitado el aumento de las medidas de seguridad "preventivas" a escala global, medidas que son implementadas muchas veces sin conocimiento ni consentimiento de las personas afectadas, y que tienen un gran impacto en los derechos y libertades fundamentales, particularmente para la dignidad y la libre autodeterminación de las personas.[1]

[1] Para corroborar lo anterior, basta pensar en los últimos escándalos sobre las revelaciones de espionaje hechas tanto por *wikiLeaks*, como por el exempleado de la CIA, Edward Snowden. En junio de 2013, Snowden hizo públicos, a través de los periódicos *The Guardian* y *The Washington Post*, documentos clasificados como alto secreto sobre varios programas de la Agencia de Seguridad Nacional norteamericana (NSA), incluyendo los programas de vigilancia masiva PRISM y XKeyscore. Al respecto véase:
http://www.wikileaks.org/wiki/WikiLeaks:About [consultado el 31.1.2014];
http://internacional.elpais.com/internacional/2010/07/26/actualidad/1280095206_850215.html [Consultado el 31.1.2014].
http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1 [Consultado el 31.1.2014]

Ante esta realidad, el derecho fundamental a la protección de datos personales, también denominado autodeterminación informativa, libertad informática o *habeas data*, se ha transformado en los últimos lustros en uno de los medios idóneo para proteger a los ciudadanos frente a los posibles abusos o externalidades negativas derivadas de uso intensivo y extensivo de las tecnologías de la información y las comunicaciones. Lo que busca este derecho es la tutela de la propia identidad informática, esto es, la posibilidad de controlar la obtención, tenencia, tratamiento y transmisión de datos relativos a su persona, decidiendo en cuanto a los mismos, las condiciones en que dichas operaciones pueden llevarse a cabo.[2]

El proceso evolutivo y de consagración de este nuevo Derecho Constitucional, no ha estado exento de polémica. Se cuestionó en su origen tanto su carácter autónomo, como la función que cumplía respecto de otros derechos fundamentales. Lo anterior queda de manifiesto en el análisis del proceso de configuración del derecho a la intimidad, tanto en el sistema norteamericano como en el continental europeo. En efecto, desde fines del siglo XIX y ante la intromisión que significaba en vida de las personas la invención de una nueva técnica que permitía captar fotografías sin pedir el consentimiento del retratado, se plantea por primera vez el nacimiento un nuevo derecho: el derecho a la privacidad.[3] La novedad de este nuevo derecho radica en que cambia el eje de la argumentación respecto al fundamento tradicional del mismo. De una concepción civilista, donde la propiedad era fundamento de todos los derechos, se pasa a una concepción *uisnaturalista* donde la dignidad y el libre desarrollo de la personalidad pasan a ser el soporte del mismo. Luego, estas ideas serán reformuladas para adecuarlas y servir de defensa jurídica ante los fenómenos sociales disfuncionales derivados, primero de la informática y luego, de Internet.

---

[2] Al respecto, véase María Mercedes SERRANO PÉREZ, *El derecho fundamental a la protección de datos. Derecho español y comparado* (Madrid: Civitas, 2003), pp. 67 y ss. Para la evolución de dicho concepto, véase Vitorio FROSINI, "Banco de datos y tutela de la persona", *Revista de Estudios Políticos* vol. 30 (1982), p. 24; Vittorio FROSINI, *Informática y derecho* (Bogotá: Temis, 1988), p. 110; Vittorio FROSINI, "La protezione della riservatezza nella societá informática", en *Privacy e banche dei dati*, de N. MATERUCCI (Bologna, 1981), pp. 37 y ss.; Antonio Enrique PÉREZ LUÑO, "Informática y libertad", *Revista de Estudios Políticos* n° 24 (1981): pp. 31 y ss.; Stefano RODOTÀ, *Elaboratori elettronici e controllo sociale* (Bolonia: Il Mulino, 1973), pp. 5–14. En la doctrina chilena, véase Raúl ARRIETA CORTÉS y Carlos REUSSER MONSÁLVEZ, *Chile y la protección de datos personales ¿están en crisis nuestros derechos fundamentales?* (Santiago de Chile: Universidad Diego Portales, 2009).

[3] S. D. WARREN y L. D. BRANDEIS, "The Right to Privacy", *Harvard Law Review* vol. IV, n° 5 (15 de diciembre de 1890).

Dichas ideas pasarán al continente europeo, derivando en lo que conocemos actualmente como el derecho fundamental a la protección de datos personales. Desde la labor pionera desarrollada por el Consejo de Europa a partir de la década de los sesentas, hasta la consagración definitiva de la protección de datos personales como derecho fundamental autónomo en el artículo 8º de la Carta Europea de Derechos Fundamentales, a principios del presente siglo, se puede ver la evolución y adaptación de este derecho. Actualmente, éste derecho cuenta con un conjunto de principios esenciales bien definidos, derechos y obligaciones claras, así como el establecimiento de autoridades de control independientes que garantizan el efectivo cumplimiento de las normas a nivel estatal y europeo.

Lo anterior, es plenamente válido, por lo menos, para lo que se denomina antiguo primer pilar comunitario, pero dicha afirmación no puede aplicarse en forma categórica respecto del ámbito referido a la cooperación policial y judicial en materia penal (antiguo tercer pilar).[4] En efecto, el principal instrumento jurídico sobre la materia es 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 éstos. Dicha Directiva se aplica a todas las actividades de tratamiento de datos personales en los Estados miembros tanto en el sector público como en el privado. No obstante, ella no se aplica al tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como lo son las actividades de cooperación judicial en materia penal y de la cooperación policial, ámbito conocido antiguamente como tercer pilar comunitario.

El marco jurídico actual de la protección de datos en materia de prevención y represión penal en la Unión Europea, se configura a través de un entramado de normas dispersas y aisladas por áreas específicas (v.g. Europol, Eurojust, Sistema de Información Schengen, Sistema de Información de Visados, entre otros). A lo anterior,

[4] El Tratado de Maastricht (1992) introdujo una nueva estructura institucional a la Unión Europea que se mantuvo hasta la entrada en vigor del Tratado de Lisboa. Dicha estructura institucional estaba compuesta por tres «pilares». El primer pilar (comunitario), correspondía a las tres comunidades: la Comunidad Europea, la Comunidad Europea de la Energía Atómica (Euratom) y la antigua Comunidad Europea del Carbón y del Acero (CECA); el segundo pilar, correspondiente a la política exterior y de seguridad común, que estaba regulada en el título V del Tratado de la Unión Europea; y el tercer pilar correspondiente a la cooperación policial y judicial en materia penal, cubierta por el título VI del Tratado de la Unión Europea.

se suman las denominadas "cooperaciones reforzadas", materializadas en algunos acuerdos o tratados internacionales suscrito entre algunos miembros de la Unión.[5] Todo ello ha impedido el desarrollo coordinado y homogéneo de un *corpus* normativo claro sobre protección de datos en el ámbito de la cooperación policial y judicial en materias penales.

Con el fin de superar dichas falencias y contar con un instrumento equivalente a la Directiva 95/46/CE en el antiguo tercer pilar comunitario, se dictó 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. No obstante, éste instrumento no cumplió con la finalidad de aunar criterios y servir como estándar mínimo a respetar en el tratamiento de datos personales en el ámbito de la prevención y represión penal, atendido su limitado ámbito de aplicación. En efecto, la Decisión Marco excluye de su esfera de aplicación el tratamiento realizado al interior de cada Estado por parte de las policías nacionales o locales (tratamiento domestico), como también el tratamiento realizado por parte de autoridades competentes a efectos de prevención y represión penal en actos de la Unión que regulen el tratamiento de datos personales, tales como Europol y Eurojust. Así mismo, excluye de su ámbito de aplicación el acceso a los sistemas de información establecidos en el ámbito de la cooperación policial y judicial, como los Sistemas de Información Schengen (SIS) y el Sistema de Información de Visados (SIV), entre otros. Por tanto, la citada Decisión Marco no puede ser considerada el marco de referencia general y supletoria para éste tipo de tratamiento de datos personales.

Con la entrada en vigor del Tratado de Lisboa y la progresiva desaparición de los antiguos pilares que regían la arquitectura normativa de la Unión Europea, se ha dado un nuevo impulso a la regulación de la protección de datos personales en el ámbito de la cooperación judicial y policial. Prueba de ello, es la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos.[6] Esta

[5] Un ejemplo claro en este sentido lo constituye el Tratado de Prüm.
[6] COM (2012) 10 final, del Parlamento Europeo y del Consejo, de 25.1.2012.

Propuesta, que pretende derogar y sustituir a la Decisión Marco 2008/977/JAI, si bien se hace cargo de algunas de las críticas formuladas a ésta, al incluir dentro de su ámbito de aplicación los tratamiento domésticos de datos personales realizados por la órganos competentes de los Estados miembros, mantiene la dispersión y atomización normativa. En efecto, la Propuesta excluye de su ámbito de aplicación los tratamientos de datos realizados por organismos europeos tales como Europol y Eurojust, así como también, los tratamientos realizados por los grandes sistemas de tratamiento de información en el ámbito penal europeo, tales como SIS y SIV, entre otros. En consecuencia, de aprobarse la Propuesta de Directiva sin las modificaciones pertinentes, se perpetuarían gran parte de los problemas criticados a la Decisión Marco que pretende sustituir.

Uno de los principales problemas con que se enfrenta la normativa europea sobre protección de datos personales es la transferencia internacional de éstos a terceros países u organismos internacionales. Ello, porque muchas veces los principios, derechos y obligaciones reconocidos y sancionados por la Unión Europea no están presentes o lo están en menor medida o de manera diversa en terceros Estados. Además, cuando los datos personales circulan a través de las fronteras se puede poner en riesgo la capacidad de las personas físicas para ejercer las facultades que otorga el derecho a la protección de datos, disminuyendo la posibilidad de controlar la utilización ilícita de dichos datos. Al mismo tiempo, es posible que las autoridades de control se vean en la imposibilidad de tramitar reclamaciones o realizar investigaciones relativas a actividades desarrolladas fuera de sus fronteras. También, los esfuerzos por colaborar en el contexto transfronterizo pueden verse obstaculizados por poderes preventivos o correctores insuficientes y regímenes jurídicos incoherentes. Por tanto, junto con fomentar una cooperación más estrecha entre las autoridades de control de la protección de datos, para ayudarles a intercambiar información con sus homólogos extranjeros, es necesario reforzar el ejercicio de los derechos esenciales inherente a la protección de datos personales.

Un ejemplo de lo señalado son los problemas suscitados entre EE.UU. y la UE por la obligación que imponían las leyes antiterroristas norteamericana (*Patriot Act*) dictadas inmediatamente después de ocurridos los atentados a los torres gemelas del 11-S. En este trabajo analizamos en particular una de estas medidas: la que imponía a todas las compañías aéreas la obligación de entregar todos los datos personales consignados

en los registros de nombre de pasajeros (*Passenger Name Record, PNR*) que gestionan líneas aéreas con destino, escala o que sobrevolaran territorio norteamericano.

Creemos que el presente trabajo de investigación se justifica ante la constatación de que, pese a los avances logrados en materia de la protección de datos personales en el ámbito de la cooperación policial y judicial, aún subsisten importantes problemas. En concreto, aún no se ha resuelto el aparente conflicto entre la necesidad de conciliar el ejercicio efectivo de los principios y derechos inherentes a la protección de datos personales, con la necesidad de dotar a los organismos públicos encargados de la prevención y represión penal de los medios idóneos, incluido el tratamiento de datos personales, para el cumplimiento de sus fines. La adecuada ponderación y equilibrio entre los interese en juego es la clave que guía este trabajo.

3. Objeto de la investigación

El objetivo general de esta tesis es realizar un análisis de algunos aspectos relevantes del derecho fundamental a la protección de datos personales en el ámbito específico de la cooperación policial para la prevención y represión penal en el derecho europeo.

Los objetivos específicos que guían el presente trabajo son: revisar el origen y evolución del derecho fundamental a la protección de datos personales en el sistema norteamericano; examinar la forma cómo se ha construido el derecho fundamental a la protección de datos en el sistema continental europeo, particularmente en Alemania, Italia y España; establecer cuáles son las principales directrices a nivel internacional sobre el derecho fundamental a la protección de datos personales; determinar cuál es el marco normativo actualmente vigente para la regulación del derecho fundamental a la protección de datos en el ámbito de prevención y represión penal; precisar quiénes son los posibles afectados (interesados) con este tipo de tratamiento de datos, así como determinar cuáles son sus derechos y los límites justificados a la restricción de los mismos; revisar críticamente las condiciones bajo las cuales se permite la transferencia internacional de datos a terceros países y organismo internacionales; y realizar un análisis crítico de los acuerdos internacionales suscritos por la Unión Europea con

terceros Estados a objeto de transferir o permitir el acceso a los datos personales contenidos en el registro de pasajeros que gestionan las compañías aéreas (PNR) por parte de los organismos de seguridad.

4. Enfoque metodológico

El método utilizado en esta investigación es esencialmente bibliográfico. Se utilizó respecto del material seleccionado el análisis deductivo, inductivo, analítico, sintético, comparativo o analógico, histórico, dialéctico y exegético.

Las fuentes consultadas son mayoritariamente legislación, doctrina y jurisprudencia pertinente sobre la materia. Se revisó la legislación sobre protección de datos personales a nivel internacional y europeo, poniendo especial énfasis en las normas vinculadas al tratamiento de datos personales con fines de prevención y represión penal. También se consultó la bibliografía especializada, constatando la escasa doctrina que existe en castellano sobre el tema que abordamos. Además, se consultaron algunos de los principales fallos tanto del Tribunal Europeo de Derecho Humanos, como del Tribunal de Justicia de la Unión Europea, y algunos fallos relevantes de los Tribunales Constitucionales de Alemania y España.

5. Contenido de la investigación

La tesis se ha dividido en tres partes: en la primera se revisan los elementos dogmáticos más importantes que han permitido la construcción del derecho a la protección de datos como un nuevo derecho fundamental; la segunda, se destina a determinar el marco jurídico general y específico aplicable al tratamiento de datos personales en el ámbito de la cooperación policial; y la tercera, centra el análisis en dos aspectos críticos del tratamiento de datos con fines de prevención y represión penal: los interesados y sus derechos, y las transferencias internacionales de datos personales.

La primera parte se ha divido a su vez en tres capítulos. En el capítulo primero, se realiza una pequeña síntesis del origen y evolución del derecho a la *privacy* en Estados Unidos de Norteamérica, partiendo desde las primeras elaboraciones

doctrinarias realizadas por los juristas Warren y Brandeis a fines del siglo XIX, siguiendo con las transformaciones que se han formulado a este derecho para adecuarlo a los peligros derivados del procesamiento de datos por medio de la informática, y terminando con los problemas que presenta la protección de datos en la actualidad con Internet.

El capítulo segundo, se dedica a revisar la construcción del derecho fundamental a la protección de datos en tres países de Europa: Alemania, Italia y España. Su elección se debe a que en todos ellos se ha producido un desarrollo legislativo, dogmático y jurisprudencial que les ha permitido, a lo largo de los últimos treinta años, configurar la protección de los datos de carácter personal como un nuevo derecho fundamental. Si bien los tres países han abordado el tema de formas distintas, los argumentos construidos para la defensa de este nuevo derecho constitucional poseen elementos comunes, que es necesario desatacar. Ello nos permitirá tener claro cuáles son los presupuestos conceptuales sobre los cuales se articula la construcción del derecho a la autodeterminación informativa o protección de datos personales.

El capítulo tercero, se destina al análisis de las directrices internacionales en materia de protección de datos personales. Se revisan particularmente las recomendaciones de la Organización para la Cooperación y Desarrollo Económico (OCDE); las directrices de la Organización de Naciones Unidas (ONU) para la regulación de los archivos de datos personales informatizados; y las directrices del Foro de Cooperación Económica Asia-Pacifico (APEC). Asimismo, se propone la necesidad de un instrumento jurídico universal vinculante en la materia, tomando como base los estándares internaciones existentes.

La segunda parte de la tesis se destina al análisis del marco jurídico aplicable a la protección de datos. Para ello realizamos una primera distinción entre las normas que tienen su fuente en el Consejo de Europa y las que provienen de la Unión Europea. Por ello, el capítulo cuarto se destina al estudio de las principales normas del Consejo de Europa con incidencia en el objeto de nuestro estudio; el capítulo quinto al estudio de las normativa general sobre protección de datos; y el capítulo sexto se destina a las normas específicas o con incidencia directa en el tratamiento de datos personales con fines de prevención o sanción penal.

Por último, la tercera parte de la tesis se destina al análisis crítico de dos aspectos centrales para el tratamiento de datos personales en el ámbito de la cooperación policial con fines de prevención o represión penal. El capítulo séptimo se dedica a lo que hemos denominado ámbito subjetivo del tratamiento de datos personales, donde se ve quienes son los titulares (interesados) cuyos derechos pueden verse afectados, los derecho y las condiciones para su ejercicio, así como los límites a los mismos. Por último, en el capítulo octavo, se estudia detalladamente la normativa actual y las eventuales modificaciones que se quieren introducir a las transferencias internacionales de datos personales con fines de sanción o prevención penal. Así mismo, en éste último capítulo se realiza un estudio de un caso crítico sobre transferencias internacionales de datos: los acuerdos suscritos por la Unión Europea con terceros Estados sobre transferencia de datos personales contenidos en los registros de nombres de pasajeros (PNR), contenidos y gestionados por las líneas aéreas.

Por último, queremos dejar constancias de las limitaciones y exclusiones de ésta investigación. En primer lugar, queremos señalar que si bien en ella se realiza una primera aproximación histórica desde el derecho comparado, el eje principal del análisis se centra temporal y espacialmente en la normativa europea aprobada con posterioridad al año 2001. La elección de éste periodo se debe esencialmente a la irrupción de un nuevo tipo de terrorismo, de corte global e integrista, cuyas manifestaciones más tangibles fueron los atentados en Nueva York en 2001,en Madrid en 2004 y en Londres en 2005 y que trajo como consecuencia modificaciones legislativas importantes para hacer frente a dicho flagelo, lo que redundó en una evidente y sostenida limitación de algunos derechos y libertades individuales, entre las que sin duda uno de los mayores afectados fue el derecho fundamental a la protección de datos.

Por otra parte, por razones de tiempo y presupuesto, se tuvo que optar por seleccionar ciertos aspectos del tratamiento de datos personales para ser analizados con mayor profundidad, dejando para un eventual investigación posterior otros aspectos no menos relevantes, como por ejemplo: la adecuada ponderación entre de los principios rectores de la protección de datos con el principio de disponibilidad que rige la labor policial europea; analizar el funcionamiento de los sistemas jurisdiccional y administrativos existentes destinados a garantizan el ejercicio efectivo del derecho a la

protección de datos en Europa; y determinar cómo se ha afectado los datos especialmente protegidos o sensibles con el tratamiento de datos en el ámbito de la cooperación policial europea.

Otra limitación importante en este proceso de investigación, fue la ausencia de estudios monográficos dedicados al tema, sobre todo en lengua castellana. Esperamos, por tanto, que este trabajo se constituya en un primer y pequeño aporte para el desarrollo de investigaciones futuras en ésta área específica del derecho.

PRIMERA PARTE

ORIGEN, EVOLUCIÓN Y CONSOLIDACIÓN DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS

CAPÍTULO PRIMERO
ORIGEN Y EVOLUCIÓN DE LA PRIVACY EN NORTEAMERICA

SUMARIO: 1. LA PRIMERA FORMULACIÓN DOCTRINAL DE LA *PRIVACY* (WARREN Y BRANDEIS); 2. LA REFORMULACIÓN DE LA *PRIVACY* EN LOS INICIOS DE LA INFORMÁTICA; 3. LA *PRIVACY* EN LA ERA DE INTERNET.

INTRODUCCIÓN

Para comprender adecuadamente el derecho a la protección de datos personales, resulta esencial una primera aproximación metodológica desde el Derecho comparado.[7] Ello nos permitirá contextualizar las necesidades sociales en las cuales ha surgido y desarrollado esta institución jurídica, y conocer cuál ha sido la respuesta dogmática, legal y jurisprudencial ante tales desafíos.[8]

Iniciamos el estudio del presente apartado analizando brevemente la doctrinal norteamericana más relevante, por ser ella la que da inicio a la discusión sobre la existencia de un nuevo derecho con perfiles propios: la intimidad. Estos planteamientos doctrinarios sentarán las bases para el desarrollo y construcción de la tutela de este derecho por parte del Tribunal Supremo de los Estados Unidos, para posteriormente recibir reconocimiento normativo. Acotando el objeto de estudio, nos centraremos en lo que denominamos contenido esencial de la *privacy* en la dogmática norteamericana, desde un punto de vista *iusfundamental*.[9]

---

[7] Al respecto véase los libros monográficos de Ricard MARTÍNEZ MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa* (Madrid: Thomson-Civitas, 2004); y María Mercedes SERRANO PÉREZ, *El derecho fundamental a la protección de datos. Derecho español y comparado*, (Madrid: Civitas, 2003).

[8] Como señala Richard MARTÍNEZ, «la determinación del contexto en que nacen y posteriormente evolucionan las instituciones jurídicas siempre aportan respuestas desde el punto de vista práctico», ya que permiten conocer el contexto social y jurídico en que se gestó un derecho, los problemas que con él se trataron de resolver y las soluciones y aplicaciones constitucionales, legales y jurisprudenciales que se derivaron de él». Cfr. op. cit., p. 61.

[9] Se excluye, por tanto, el estudio de la protección civil de la intimidad en Norteamérica por la vía del «*tort*». En este punto seguimos a Ricard MARTÍNEZ, para quien el empleo del término «*tort*» contextualiza claramente el derecho a la vida privada en el marco de los litigios civiles y, por tanto,

1. LA PRIMERA FORMULACIÓN DOCTRINAL DE LA PRIVACY (Warren y Brandeis)

Hasta fines del siglo XIX la vida privada no fue objeto de especial protección jurídica en el ámbito anglosajón. Bajo una óptica eminentemente liberal, donde la propiedad era considerada el origen de todos los derechos, las amenazas a la vida privada, eran entendidas como incursiones de terceros en el ámbito territorial propio.[10]

Bajo esta lógica, bastaba para la defensa jurídica de la privacidad invocar la afectación del derecho a la propiedad mediante los recursos que ofrecía el sistema. La defensa y tutela de la vida íntima aparecían como una forma de tutela de un ámbito físico o territorial sobre el cual se ejerce propiedad.[11] Ello explica que los derechos constitucionales reconocidos en relación a la intimidad fueran la inviolabilidad del domicilio y de la correspondencia, los cuales obedecían al deseo de proteger al individuo frente a la amenaza que proviene del Estado.

El cambio de paradigma que hemos señalado, se produce con la célebre obra de Warren y Brandeis.[12] Ellos plantean por primera vez el derecho a la intimidad como un derecho de naturaleza constitucional vinculado a la tutela de la dignidad de individuo.

El origen y motivación de su artículo fue un problema que afectaba a uno de sus autores.[13] La pregunta que se formularon fue si el *Common Law* ofrecía alguna

---

alejado de la tutela de los derechos fundamentales. Cfr. op. cit., p. 74. Para una definición de la voz «*tort*», véase *The lectric Law Library's Lexicon On,* disponible en *http://www.lec-tlaw.com/def.htm*

[10] Al respecto John LOCKE, señalaba que «aunque las cosas de la naturaleza son dadas en común, el hombre, al ser dueño de sí mismo y propietario de su persona y de las acciones y trabajos de esta, tiene en sí mismo el gran fundamento de la propiedad». Cfr. *Segundo Tratado sobre el Gobierno Civil*, trad. C. Mellizo, Alianza Editorial, Madrid, 1994, Nº 44, p. 70. En la misma línea, Hernán CORRAL TALCIANI, «Configuración jurídica del derecho a la privacidad I: origen, desarrollo y fundamentos», *Revista Chilena de Derecho*, Santiago de Chile, Vol. 27, Nº 1, 2000, p. 53.

[11] De allí la máxima que se acuña en el derecho anglosajón *a man's house is his castle* (la casa del hombre es su castillo). Al respecto véase, Hernán CORRAL TALCIANI, op. cit., p. 51.

[12] S. D.WARREN y L. BRANDEIS: «The Right to *Privacy*», *Harvard Law Review*, vol. IV, núm. 5, 15-12-1890. Existe traducción al español: WARREN S. D. y BRANDEIS, L.: *El derecho a la intimidad* (Benigno Pendas y Pilar Baselga ed.), Civitas, Madrid, 1995.

[13] Warren se había casado con la hija de un Senador. Debido a la proyección social de su matrimonio se vio sometido al acoso de la prensa ávida de «chismes» o como se le llama eufemísticamente «ecos de sociedad» y se sintió indefenso ante el avance tecnológico que para aquel tiempo representaba la

respuesta frente a las intromisiones en la vida privada por parte de la prensa escrita. Esta intromisión se refería particularmente a dos fenómenos: el desarrollo de la industria periodística dedicada al chisme y la aparición de un nuevo invento, que ellos denominan en su trabajo «la fotografía instantánea». Con esta nueva tecnología, al no ser necesario solicitar al personaje una pose para retratarlo, se sustraía del conocimiento del mismo el hecho de ser observada y en consecuencia de cualquier control sobre su información privada.[14] La *privacy* surge entonces como un intento de freno frente al inmenso poder de intromisión desarrollado entonces por la prensa estadounidense.[15]

La aproximación de los autores al tema fue eminentemente empírica, buscando una solución jurídica a una nueva categoría de conflictos. Lo relevante del trabajo de Warren y Brandeis, está en que elaboran una teoría que altera sustancialmente la tutela de algunos derechos de la personalidad, al trasladar el centro de gravedad de la cuestión desde una tutela construida sobre los cimientos de la propiedad privada a una nueva construcción cuyo fundamento es la dignidad del hombre y la inviolabilidad de la personalidad humana.[16]

El método utilizado por los autores para dar respuesta el problema fue analizar las soluciones que hasta ese momento se ofrecían en el derecho norteamericano ante este tipo de conflictos, delimitando las instituciones jurídicas que podrían aplicarse al

---

fotografía instantánea, la cual, permitía a los periodistas captar subrepticiamente imágenes y publicarlas posteriormente sin conocimiento ni consentimiento de la persona retratada.

[14] Aun cuando han transcurrido más de 120 años desde la publicación de la obra de Warren y Brandeis, coincidimos con Ricard Martínez, en que, varios pasajes, resultan muy esclarecedores y de gran actualidad, como los que transcribimos a continuación: «Los recientes inventos y los métodos de hacer negocios fueron focos de atención en el siguiente paso que hubo de darse para amparar a la persona, y para garantizar al individuo lo que el juez Cooley denomina el derecho "a no ser molestado" [*the right to be let alone*]. Las empresas periodísticas han invadido los sagrados recintos de la vida privada y hogareña; y los numerosos ingenios mecánicos amenazan con hacer realidad la profecía que reza: "lo que se susurre en la intimidad, será proclamado a los cuatro vientos (…) La intensidad y la complejidad de la vida, que acompañan a los avances de la civilización han hecho necesario un cierto distanciamiento del mundo, y el hombre, bajo la refinada influencia de la cultura, se ha hecho más vulnerable a la publicidad, de modo que la soledad y la intimidad se han convertido en algo esencial para la persona; por ello los nuevos inventos, al invadir su intimidad, le producen un sufrimiento espiritual y una angustia mucho mayor que la que le pueden causar los meros daños personales». Véase, S. D. WARREN y L. BRANDEIS: «The Right to Privacy», op. cit., p. 25-27 y Ricard MARTÍNEZ, op. cit., p. 67.

[15] En el mismo sentido véase María Mercedes SERRANO PÉREZ, *El derecho fundamental a la protección de datos. Derecho español y comparado,* Civitas, Madrid, 2003, p. 29; Vitorio FROSINI, «Banco de datos y tutela de la persona», *Revista de Estudios Políticos,* vol. 30, Nueva Época, 1982, p. 21; y Piero MONNI, *L' informaciones: un diritto, un devere,* Internazionale, Cagliari, 1989, p. 158.

[16] Ricard MARTÍNEZ, señala que el mérito de la obra de Warren y Brandeis, reside en buscar una solución o, si se prefiere, una reinterpretación del Derecho en un contexto tecnológico a la vez que lo cimentan sobre bases completamente nuevas. Cfr. *Una aproximación crítica…,* op. cit., p. 68.

supuesto de hecho objeto de análisis. Parten por el estudio del derecho a no ser molestado *(right to be let alone)* planteado por el juez Cooley un par de años antes.[17] Luego estudian los derechos reconocidos por la ley de difamación y libelo, descartando su aplicación al caso en estudio por tener un objeto diferente, que sería la consideración externa del individuo en la comunidad y los daños materiales que con su vulneración se provocarían.[18]

De esta forma, llegan a la siguiente conclusión: lo que caracterizaría la nueva realidad que se pretende describir sería la facultad del individuo de ejercer un cierto control sobre su vida privada. A ello apuntan los autores cuando señalan que el *Common Law* garantiza a cada persona el derecho a decidir hasta qué punto pueden ser comunicados a otros sus pensamientos, sentimiento y emociones.[19]

Con estos argumentos se traslada la tutela del derecho a la intimidad desde el plano de la propiedad al ámbito del derecho a la personalidad.[20] Así, el fundamento de este derecho no estaría en el derecho de propiedad sino en la inviolabilidad y dignidad del ser humano.[21]

---

[17] Thomas COOLEY, *Treatise on the Law of Torts* (Chicago: Callaghan & Company, 1888). Estamos de acuerdo con la traducción realizada por Pilar Baselga, del «right to be let alone» como «derecho a no ser molestado», en vez de una más literal, como sería «derecho a ser dejado solo», ya que la primera da cuenta de la realidad jurídica que pretende describir. En el mismo sentido Ricard MARTÍNEZ, agrega que en el texto [de WARREN y BRANDEIS] el derecho a la vida privada tutela al individuo frente a un conjunto de conflictos cuyo nexo común consiste precisamente en la protección frente a distintas perturbaciones externas. Cfr. *Una aproximación crítica…,* op. cit., p. 69.

[18] «El principio en que se basa dicha ley de difamación abarca un tipo de consecuencias radicalmente diferentes (…). Esta contempla solamente los perjuicios causados a la reputación, los daños causados al individuo en sus relaciones externa con la comunidad, al hacerle perder la estima de sus conciudadanos (…), para que haya lugar a la demanda por difamación lo que se hace público sobre una persona debe tener la intensión directa de perjudicarle en su relación con otros, y, por tanto en lo escrito como en lo publicado, debe hacerle objeto del odio, del ridículo o del desprecio de sus conciudadanos —el efecto que puede tener lo publicado en su propia estima y en sus sentimientos no constituye un elemento esencial en el fundamento de la acción—. En resumen, los daños y los correspondientes derechos reconocidos por la ley de difamación y libelo son, por su naturaleza, más bien materiales que espirituales». Véase WARREN y BRANDEIS: *El derecho a la intimidad…,* op. cit., pp. 28-29.

[19] Ricard MARTÍNEZ, *Una aproximación crítica…,* op. cit., p. 70.

[20] Ibídem, p. 71.

[21] Lo anterior queda de manifiesto en el siguiente párrafo: «Por tanto, llegamos a la conclusión de que los derechos así tutelados, cualquiera sea su exacta naturaleza, no emanan de un contrato o de una especial buena fe, sino que son derechos *erga omnes*, y como se dijo anteriormente, el principio que se ha aplicado para amparar estos derechos no es en realidad el principio de propiedad privada, por más que esa palabra sea empleada en sentido amplio y poco usual. El principio que tutela los escritos personales y cualquier otra obra producto del espíritu o de las emociones es el derecho a la intimidad, y el derecho no necesita formular ningún principio nuevo cuando hace extensivo este amparo a la apariencia personal, a los dichos, a los hechos y a las relaciones personales, domésticas o de otra clase». Véase Samuel D. WARREN y Louis D. BRANDEIS, *El derecho a la intimidad*, ed. Benigno PENDAS y Pilar BASELGA (Madrid: Civitas, 1995), p. 59.

Con su trabajo Warren y Brandeis, configuran el derecho a la intimidad como un derecho de contenido amplio, que incorporaba facultades de control sobre las propias informaciones. **Su gran mérito sería, por una parte, haber definido los elementos esenciales del derecho, y por otra, haberlo concebido como un derecho de textura abierta y naturaleza fundamental, trasladando su fundamento desde el paradigma del derecho de propiedad a la inviolabilidad y dignidad del ser humano, es decir, al ámbito del derecho a la personalidad**.[22] De esta forma se supera la formulación originaria de la *privacy* como un derecho de contenido negativo, individualista y de estructura semejante al derecho de propiedad.[23]

Los planteamientos de Warren y Brandeis, no fueron unánimemente aceptados por la doctrina norteamericana y dieron lugar a distintos debates.[24] Así, Prosser[25], señala que la *privacy* no es un fenómeno aislado sino que esconde cuatro tipos distintos de agravios *(«tort»)*. Estos serían: la intrusión en la soledad, retiro, o en los asuntos privados; la difusión pública de hechos privados; la información que da una imagen falsa del afectado ante los ojos del público *(«False light»)* y, por último, la apropiación en beneficio propio de la imagen o el nombre ajenos. El elemento común en todos ellos es la afectación del derecho a ser dejado en paz. Luego del análisis detallado de cada uno de ellos, el autor concluye que, «puesto que cada uno de los cuatro supuestos pueden darse independiente o conjuntamente con los demás, lo que ha sucedido es que

[22] Ricard MARTÍNEZ, *Una aproximación crítica…,* op. cit., p. 73.

[23] Vittorio FROSINI, señala que "la doctrina propuso y discutió varias veces la comparación entre el derecho a la privacidad, invocado por el hombre de nuestro siglo [Siglo XX] y el derecho a la propiedad privada en la concepción de los primeros autores WARREN y BRANDEIS. Según este autor, no se trata de un paralelismo preciso ya que el derecho a la intimidad supera la esfera del Derecho privado y la patrimonial. Cfr. «Banco de datos…», op. cit., p. 24 y Mª Mercedes SERRANO PÉREZ, *El derecho fundamental a la protección de datos*…, op. cit., p. 29.

[24] En cuanto a la discusión posterior sobre el tema en la dogmática norteamericana y la consagración de la *privacy* como derecho fundamental en la jurisprudencia del Tribunal Supremo, sólo enunciaremos someramente los principales planteamientos de los mismos, por ser una materia que ha sido objeto de estudios anteriores a los cuales nos remitimos para su profundización. Para un completo estudio sobre la discusión dogmática sobre la *privacy* desde Warren y Brandeis hasta los inicios de Internet, véase Ricard MARTÍNEZ, *Una aproximación crítica…,* op. cit., pp. 66-102. En la misma obra, se desarrolla el debate sobre la *privacy* en la jurisprudencia norteamericana (pp. 102-133).

[25] William PROSSER, "Privacy", *California Law Review* vol. 48 (1960): 383–423. Sus teorías han sido descritas con distinto éxito en la doctrina española, al respecto véase: Fernando HERRERO TEJEDOR, *La intimidad como derecho fundamental* (Madrid: Colex, 1998); y J. Mª SOUVIRÓN MORENILLA, «Privacidad y derechos fundamentales», en VVAA, *Introducción a los derechos fundamentales*, vol. III, Ministerio de Justicia, Madrid, 1998, pp. 1873-1890.

sobre un único concepto, la *privacy*, los jueces han amparado cuatro supuestos diferenciados de responsabilidad».[26]

Como respuesta a Prosser, surge la propuesta de Edwuard J. Bloustein[27], de construir una noción general del concepto de vida privada capaz de responder a los nuevos desafíos que plantea el avance científico y tecnológico. Este autor criticó la tesis de Prosser, por varias razones, como el haber desmenuzado la *privacy* en cuatro *«tort»* y, en la práctica, considerarlos como nuevos modos de cometer viejos *«tort»*. También critica su enfoque centrado en el daño (*«mental suffering»*) obviando que éste es siempre consecuencia de la vulneración de la *privacy*. Por último, critica su teoría por acercarse al derecho de propiedad, de la cual, Warren y Brandeis expresamente se distanciaron.[28]

Para Bloustein, lo fundamental es que la cultura occidental define lo individual incluyendo el derecho a estar libre de determinados tipos de intromisiones y que ello comporta un cierto control personal sobre nuestro asilamiento que integra la esencia de la libertad personal y de la dignidad. Por lo tanto, «más que fundamentar los casos de intrusión en la causación intencional de daños mentales o morales habría que referirlos a la dignidad humana, a un asalto contra la dignidad».[29]

2. LA REFORMULACIÓN DE LA PRIVACY EN LOS INICIOS DE LA INFORMÁTICA

En los albores de la informática, la discusión doctrinal sobre la *privacy* continuó en EE.UU con Westin y Fried, que contribuyeron a lo que se ha denominado la dimensión informacional de la *privacy*.[30]

Para Fried[31] lo que caracteriza realmente a la *privacy*, es la posibilidad de ejercer un control sobre la información propia tanto desde un punto de vista cuantitativo como,

[26] Cfr. Ricard MARTÍNEZ, op. cit., p. 75.
[27] Edward J. BLOUSTEIN, "Privacy as an aspect of human dignity: an answer to Dean PROSSER", *New York University Law Rewiew* vol. 39 (diciembre de 1964): 964-1007.
[28] Ricard MARTÍNEZ, op. cit., p. 76.
[29] Ídem.
[30] Ibídem, p. 78.
[31] Charles FRIED, "Privacy", *The Yale Law Journal*, vol. 77, (1967-1968): 475-493.

sobre todo, cualitativo.[32] La *privacy* juega un rol instrumental respecto de la libertad personal en la medida en que nos permite ejercer un dominio sobre el contexto. En este sentido «dominar la información que nos concierne permite definir el grado de intimidad de nuestras relaciones personales».[33]

La obra de Alan F. Westin[34], también se sitúa temporalmente a fines de los años sesenta y se centra en los distintos problemas que afectaban la vida privada en Estados Unidos. Uno de sus grandes aportes, fue la definición de privacidad en términos de autodeterminación *«self determination»*.[35] Su teoría, formula las bases de los que se denomina *«informational privacy»*.[36] En esencia, plantea que el individuo desea ejercer un control material sobre su información personal, pero este deseo de privacidad no es absoluto ya que interactúa con las normas sociales y con la voluntad de comunicación y participación. Luego de realizar distintas aproximaciones a la *privacy*, que incluye aspectos históricos, sociológicos y políticos, llega a la conclusión de que «la *privacy* cumpliría cuatro funciones para los individuos en las sociedades democráticas: la garantía de la autonomía personal —presupuesto de la libre elección—; la de liberación emocional como válvula de escape frente a presiones del sistema; la garantía de la autoevaluación en tanto que actividad intelectual y reservada que permite al individuo evaluar su experiencia; y la de garantizar una comunicación libre y limitada a aquellas personas que ofrezcan un adecuado grado de confianza y seguridad».[37]

En el mismo periodo, otro autor que contribuye a la teoría de la *«Informacional Privacy»* es Arthur R. Miller.[38] Partiendo de la dimensión informativa de la *privacy*, muestra cómo la irrupción y generalización de la informática introduce cambios

[32] Ricard MARTÍNEZ, op. cit., pp. 78-79.
[33] Charles FRIED, op. cit. pp. 487-488. Al respecto, Martínez, señala que la delimitación conceptual de la *privacy* depende del contexto, de los valores sociales imperantes en cada cultura. El área protegida por aquélla es un área convencional y son los sistemas sociales los que atribuyen importancia a esas áreas que constituyen «*privacy* sustantiva» ya que protegen intereses esenciales —como el sexo o la salud—, y otras que en cambio son contingentes y simbólicas. Cfr., *Una aproximación crítica…*, p.79.

[34] Alan WESTIN, *Privacy and Freedom*, (New York: Atheneum, 1970). La primera edición es de 1967.
[35] Al respecto, véase José Luis PIÑAR MAÑAS, "Protección de datos: origen, situación actual y retos de futuro", en *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, pp. 84 y ss.
[36] En este apartado solo enunciaremos los elementos principales de la teoría de Westin. Para profundizar en la misma, véase Ricard MARTÍNEZ, *Una aproximación crítica…,* op. cit., pp. 79-82 y la bibliografía citada por el autor.
[37] Alan WESTIN, op. cit., p. 23 y Ricard MARTÍNEZ, op. cit., p. 80.
[38] Arthur R. MILLER, "Personal privacy in the Computer Age: the challenge of a new technology and information oriented society", *Michigan Law Review*, vol. 67, (1967): 1089-1246.

significativos para la tutela de la vida privada, lo que obliga a buscar respuestas en el ordenamiento jurídico ante este nuevo fenómeno.[39] La tecnología informática relativiza los dos supuestos sobre los que se había articulado la protección de la *privacy* (la acción por difamación y la acción por invasión a la vida privada) al difuminar la frontera que los separa, lo que obliga a considerar cambios al modelo legislativo desde una perspectiva más amplia, que dé cuenta de la nueva realidad.[40]

Siguiendo una metodología similar a la de Warren y Brandeis, en el sentido de determinar si dentro de las categorías que ofrece el *Common Law* existe alguna que permita dar respuesta a la vulneración de la vida privada, en este caso, frente a la informática, Miller llega a la conclusión de que, «dada la novedad de la tecnología y lo impredecible de su evolución y consecuencias, la mejor respuesta reside en la capacidad de reacción y la flexibilización de la Administración». Para ello, termina recomendando «la creación de alguna autoridad independiente, a imagen y semejanza de la *Federal Communication Commission*, que se ocupase de modo especializado en la cuestión».[41]

3. LA PRIVACY EN LA ERA DE INTERNET

Otro salto evolutivo en el proceso de construcción y adecuación del concepto de la *privacy*, por parte de la dogmática norteamericana, vino con el desarrollo de Internet y sus consecuencias para la privacidad.

Entre los autores que han abordado el tema se encuentra Paul M. Schwartz[42] quien sitúa su análisis en las relaciones existentes entre vida privada, democracia y ciberespacio. Plantea que las tecnologías de la información en Internet afectan a la *privacy* de modos que son «dramáticamente diferentes» de cualquier otro medio previo

[39] Ricard MARTÍNEZ, op. cit., p. 81.
[40] Ibídem, p. 82.
[41] Arthur MILLER, op. cit., pp. 1236-1239 y Ricard MARTÍNEZ, op. cit., p. 82.
[42] Fred H. CATE, "Principles on Internet Privacy", *Connecticut Law Review*, 2000, pp. 877-896; Paul M. SCHWARTZ, «Privacy and Democracy in Ciberspace», en *Vanderblit Law Review*, vol. 52, 1999, pp. 1609-1701. En este apartado solo se señalaran los aspectos generales de la tesis de Schwartz, para profundizar sobre el tema véase Ricard MARTÍNEZ, *Una aproximación crítica…,* op. cit., pp. 82-90 y la bibliografía citada por el autor.

hasta el punto de que las normas que ahora se desarrollen en la materia jugarán un papel esencial en la configuración de la democracia en la era de la información.[43]

En otra obra, Schwartz analiza la relación entre la *privacy* en Internet y el Estado, examinando las consecuencias prácticas para el derecho a la vida privada a la luz de las tecnologías de la información y las comunicaciones.[44] Desarrolla su planteamiento, señalando que considerar a la *privacy* como un derecho que atribuye facultades de control sobre la información personal, comporta como correlato la atribución de un importante grado de autonomía personal. Ahora bien, si esa autonomía se concibe en términos de ausencia de regulación estatal dejando en manos de los particulares la fijación de las condiciones que deben regir en el «mercado de la *privacy*», la consecuencia no es otra que el debilitamiento del derecho y, por esta vía, la reducción del espacio de libertad. Es más, de la mano de esta concepción y en el contexto de Internet se camina hacia una mercantilización de la vida privada que estimula una visión propietaria de la *privacy* más cercana al derecho de propiedad intelectual.[45]

Como se puede apreciar Schwartz critica el paradigma dominante de la *privacy-control* basada en la autonomía del individuo y en el principio del consentimiento y lo hace a la luz de un profundo examen de las consecuencias para la vida privada derivadas de las tecnologías de la información y las comunicaciones y de las prácticas existentes en Internet.[46]

Las críticas al planteamiento de Schwartz, vienen desde las concepciones más neoliberales de la *privacy* con Fred H. Cate.[47] Este critica a Schwartz la falta de concreción respecto del papel del Estado en la configuración del *privacy* y, en

[43] Ricard MARTÍNEZ, op. cit., pp. 82-83.
[44] Paul M. SCHWARTZ, «Internet privacy and the State», en *Connecticut Law Review*, vol. 32, 2000, pp. 815-859. Citado por Ricard MARTÍNEZ, *Una aproximación crítica…,* op. cit., p. 84.
[45] Paul M. SCHWARTZ, op. cit., p. 820.
[46] Ricard MARTÍNEZ, cree que la crítica del autor, en un medio poco proclive al intervencionismo estatal como el norteamericano, reafirma porque debe buscarse un equilibrio entre la actuación normativa del Estado y la libertad individual, reservando al primero el papel de sentar las bases para el funcionamiento del mercado de la *privacy* y para estimular las conductas positivas de respeto a la intimidad de los ciudadanos. También ve, que en lo que se refiere al papel del Estado en la regulación y tutela de los derechos fundamentales, una aproximación al lenguaje «europeo». Cfr. *Una aproximación crítica…,* op. cit., pp. 89-90.

[47] Fred H. CATE, "Principles on Internet Privacy", *Connecticut Law Review*, 2000, 877–896.

particular, en la creación y mantenimiento de un «mercado de la *privacy*».[48] Señala que de hecho, la protección de la *privacy* está centrada prácticamente de modo exclusivo en la defensa frente a las intromisiones del aparato estatal y en el planteamiento de un concepto de lo privado por oposición con el ámbito de lo público en su dimensión gubernamental.[49] Agrega que la regulación del sector privado necesariamente constituiría una interferencia en la libre circulación de información, y que la protección de la vida privada tiene un coste en términos de transparencia en el mercado así como de conflicto con la libertad de expresión.[50]

Para Cate, la libre circulación de la información *(Open Information Flows)* y de los datos personales constituye la piedra angular de la sociedad democrática y de la economía de mercado y son elementos determinantes para la prestación de servicios al consumidor.[51] Subraya, finalmente, su preferencia por el principio de autodeterminación *(Self-Help)* para la solución de los problemas vinculados a la *privacy*, ya que las soluciones que provienen del mercado —lo privado— destacan por su mayor eficiencia por sobre las soluciones gubernamentales. Así, bajo esta lógica, la competencia y el mercado favorece que las empresas en su búsqueda por el cliente optimicen las soluciones que le ofrecen un mayor grado de protección.[52]

Otra parte de la doctrina, representada por Allen[53], coincide con Schwartz en señalar a la *privacy* como el paradigma del control sobre la información personal. Para esta autora, la idea de *privacy* contendría tres elementos: 1) el significado del término como control sobre el uso de los datos o la información personal; 2) una dimensión procesal como derecho o acción que permite ejercer el citado control y 3) en el plano normativo, la consideración como objetivo central de la regulación de la *privacy* la promoción del control de los individuos sobre sus datos o información personal.[54]

---

[48] Ricard MARTÍNEZ, op. cit., p 90.

[49] Ídem.

[50] Fred CATE, "Principles on Internet Privacy", op. cit., p. 886. Citado en Ricard MARTÍNEZ, *Una aproximación crítica…,* op. cit., p. 90.

[51] Ricard MARTÍNEZ, op. cit., p 91.

[52] Ricard MARTÍNEZ, transcribe algunos párrafos en inglés con algunos ejemplos que propone CATE. Véase: *Una aproximación crítica…,* op. cit., p. 91. En el original, CATE F. H., «Principles on Internet Privacy»…, op. cit., p. 890-891; y CATE F. H., *Personal information in Financial Service*, Financial Services Coordinating Council, 2000.

[53] A. L. ALLEN, "Privacy as data control: conceptual, practical and moral limits of the paradigm", *Connecticut Law Review*, nº 32 (2000): 861–875. Citado por Ricard MARTÍNEZ, op. cit., p. 92.

[54] Ricard MARTÍNEZ, op. cit., p. 92-93.

Para la profesora Allen, la ausencia de un consenso sobre el concepto de la *privacy* se debería a la confluencia de tres factores: la variedad en el uso del significado denotativo y connotativo del término, la variedad de finalidades que se le han atribuido y a la diversidad de enfoques existentes en los intentos por definirlo.[55] Para esta autora, en Norteamérica se le atribuiría a la *privacy* un concepto muy amplio vinculado a la idea de autonomía individual, en el que, sin embargo, no encaja por su estrechez la idea de control sobre los datos personales. Por ello, para resolver los problemas que surgen en el contexto de Internet, le parece más adecuada recurrir a la idea de accesibilidad o inaccesibilidad.

La idea de control se basa en conceptos como el consentimiento y la elección, no obstante, hay situaciones en que lo realmente relevante es poder decidir cuándo la información resulta o no accesible. En conclusión, para Allen la idea de *privacy* en Internet, o bien puede ser entendida como control sobre los datos *(data control)* o bien, como accesibilidad a la información.[56]

Otro autor que aborda el tema de la *privacy* en la red, entre otros temas relevantes a resolver en la misma, es Lessig.[57] Plantea que existen múltiples dimensiones normativas en la realidad, que van más allá del marco de la actuación del Estado a través de la legislación. Para este autor, la posibilidad de regular la red dependerá en gran medida de la arquitectura de la misma, que en términos informáticos denomina «el código». El factor determinante de cambio sería el comercio, ya que este requiere de una arquitectura de confianza. Para lograr dicha confianza se requiere la acción del Estado alterando o suplementando el código.

Por otra parte y como complemento de lo anterior, plantea como un prerrequisito lógico para regular las conductas en la red: que los individuos resulten *identificables*, es decir, se debe poder autenticar su identidad, entiendo por autenticación «el proceso por medio del cual se revelan aspectos de la identidad de una persona».[58] Así, el código

[55] Ídem.
[56] Ídem.
[57] Lawrence LESSIG, *El código y otras leyes del ciberespacio* (Madrid: Taurus, 2001).
[58] Ibídem., p. 68. Ricard Martínez nos transcribe un párrafo que me parece muy esclarecedor sobre la autenticación: «Partes de estos aspectos quedan desvelados porque la propia persona los hace públicos

sería un factor de regulación sobre el que puede actuar el Estado. Otra ventaja que ve LESSIG en este modelo, es que con él se facilitaría la aplicación extraterritorial del derecho.[59]

En cuanto a la vida privada en esta nueva realidad, Lessig plantea que los equilibrios tradicionales que venían protegiendo la *privacy*, ya no existen. La configuración de la red ha roto con ellos mediante distintas técnicas que permiten obtener información personal de modo inapreciable.[60] Ante esta nueva realidad, plantea que la *privacy* puede ser enfocada desde tres puntos de vista: desde una concepción utilitarista como derecho a no ser molestado o perturbado *(right to be let alone);* vincularlo con la idea de dignidad de la persona; y por último, enfocarlo como un concepto sustantivo que establezca un conjunto de límites que se impone normativamente a ciertas actuaciones del Estado.[61]

Una de las mayores preocupaciones de Lessig es la eficacia que aporta Internet a la posible monitorización de las conductas. Como en la red puede captarse todo, ello conlleva el aumento de registros, la creación de perfiles, la clasificación y normalización de las conductas. Ello podría generar discriminación y permitir manipular a las comunidades fijando diferencias entre los individuos.[62] Ante ello, el autor plantea dos vías de solución. Que la norma prohíba el escrutinio de las conductas o que el código limite tal posibilidad. Si se opta por esta última, las soluciones técnicas son diversas. El autor cree que la mejor medida es que el ordenador del usuario y el servidor web del proveedor de información, negocien a partir de perfiles de privacidad preestablecidos.[63] Para ello se requeriría de un software que incorporara una definición

---

otros, en cambio, quedan desvelados independientemente de la voluntad de su poseedor. La autenticación perfecta conlleva que los demás, llegasen a saber absolutamente todos los hechos relativos a uno mismo; la felicidad, por el contrario, proviene de que los demás sepan de uno bastante menos (…) en el espacio real una buena parte de nuestra identidad queda desvelada independientemente de nuestra voluntad». Citado por Ricard MARTÍNEZ, *Una aproximación crítica…,* op. cit., p. 94.

[59] Ídem.

[60] Ídem.

[61] Ibídem, pp. 94-95.

[62] Ídem.

[63] Ibídem, p. 96.

del nivel de privacidad asumido por el titular de los datos y negociara el acceso a los datos personales durante la navegación.[64]

La ley regularía el derecho de propiedad sobre la información personal permitiéndole poner «precio» a la privacidad e incorporar los límites derivados de la jurisdicción concreta en la que resida el usuario. La existencia de un marco legal definido clarificaría la actuación de los operadores jurídicos y permitiría el juego en el mercado entre aquellos que desean mayor privacidad y aquellos dispuestos a renunciar a ella.[65]

La idea de *«privacy-control»* planteada por Lessig, ha sido calificada por Schwartz de individualismo normativo. Las principales críticas son, por una parte que desconoce la presencia de obstáculos y restricciones al proceso de toma de decisiones en Internet lo que hace poco viable la corriente que sigue el mercado en la materia.[66] Por otra parte, se le critica que el modelo propietario podría interferir con las necesidades que tiene la Administración para desempeñar tareas como la atribución de beneficios y prestaciones sociales, la garantía —en el plano de la seguridad pública— de un orden democrático de convivencia o la eficacia en el funcionamiento del sistema económico.[67]

Luego del estudio de los postulados de Lessig, Schwartz, completa su modelo con la idea de fomentar las prácticas de transparencia informativa *(fair information practices)* como herramienta para proteger la privacidad en Internet. Para ello, plantea cuatro acciones: 1) la creación de obligaciones claramente definidas incluso normativamente sobre el uso de la información personal; 2) el uso de procesos informáticos comprensibles para el usuario; 3) la atribución de derechos a los individuos y 4) el establecimiento de mecanismos de vigilancia efectiva sobre el uso de los datos, ya sea a través de acciones procesales privadas, ya sea mediante algún tipo de seguimiento público o privado o a través de alguna combinación de ambas

[64] Lawrence LESSIG, op. cit., pp. 296 y ss. Ricard Martínez, señala que este software, de hecho ya existe, se trata de la Plataforma de Preferencias de privacidad conocida por el acrónimo de P3P. Cfr. Ricard MARTÍNEZ, *Una aproximación crítica…,* op. cit., p. 96
[65] MARTÍNEZ, Ricard, *Una aproximación crítica…,* op. cit., p. 96
[66] Ibídem, p. 97.
[67] Ídem.

posibilidades.[68] Schwartz, concluye que su planteamiento sería menos invasivo que el de Lessig, ya que permitiría negociar de acuerdo a las reglas de mercado el grado de privacidad que cada individuo quiere tener en Internet, pero respetando un estándar mínimo establecido normativamente.[69]

Ricard Martínez, comparando los modelos planteados por Schwartz y Lessig, señala que el primero, se basaría en un modelo de responsabilidad que conduciría a una responsabilidad *ex-post-facto,* esto es, el Derecho sólo actuaría una vez producida la lesión, valorando entonces y resarciendo los daños causados. En cambio, en el sistema de Lessig, la actuación se daría *ex-ante*, ya que el usuario establecería el grado de privacidad que desea y el valor que le atribuye, y a partir de este perfil, el programa informático *(software)* interactuaría con los operadores de servicios de Internet.[70]

Recapitulando brevemente lo visto sobre la evolución y debate que ha tenido la doctrina norteamericana entorno a la *privacy*, podemos señalar que su nacimiento y desarrollo está estrechamente vinculando, aunque no exclusivamente, con el avance de la tecnología —fotografía instantánea, informática, internet, etc.— El aporte que las distintas doctrinas han realizado a este derecho, reside en haber sido capaz de profundizar y matizar la configuración del mismo, en la medida que las necesidades sociales de cada tiempo lo requerían, poniendo las bases para su posterior reconocimiento normativo y jurisprudencial.

Así, el artículo de Warren y Brandeis, publicado en 1890, se adelantan medio siglo a la consagración del carácter constitucional de la *privacy* por parte del Tribunal Supremo, al ofrecer argumentos que emanan del propio *Common Law* para romper con un esquema civilista basado en el derecho de propiedad. Posteriormente Prosser, pone el acento en el aspecto procesal y las acciones para el resarcimiento de los daños en casos de afectación a la *privacy*. Blounstein, entregará una noción *iusfundamental* del *«right*

[68] Paul M. SCHWARTZ, «Beyond LESSIG'S *code* for internet privacy: Cyberspace filter, privacy-control, and fair information practices», en *Wisconsin Law Review*, 2000, pp. 779-780. Citado en Ricard Martínez, *Una aproximación crítica…,* op. cit., p. 100.
[69] Ibídem, pp. 100-101
[70] Ibídem, p. 99.

to privacy» y en la dignidad de la persona como última razón fundante de este derecho.[71]

Con la aparición de la informática, en los albores de los años 70, surge una generación de juristas (Fried, Miller y Westin) que sentarán las bases de la *«information privacy»*.[72] Con ella, la vida privada adquiere un valor cualitativamente diverso, ya que no solo se trata de una protección frente a intromisiones externas, ahora deberá satisfacer una nueva función, que el individuo disponga de un control real sobre su información personal. Dicho control garantiza un espacio de libertad y se convierte, a su vez, en un instrumento de protección del resto de los derechos.[73]

Con la llegada de Internet, Schwartz, Cate y Lessig aportan nuevos elementos al análisis de la cuestión. Schwartz, nos muestra las trampas que se esconden tras el funcionamiento de Internet y la falsa libertad de elegir en la *World Wide Web* de la mano de las cláusulas del tipo *«take it or leave it»*, y demuestra cómo el paradigma de la autodeterminación informativa carece de sentido sin una norma pública que establezca un estándar mínimo a cumplir. Cate, analiza la cuestión desde el punto de vista del funcionamiento del mercado y las necesidad de información asociadas a Internet. Finalmente Lessig, plantea la existencia de un conjunto de normas no escritas, ocultas tras el código informático, que modulan el comportamiento de las comunidades en Internet y proporcionan herramientas para el control de la información personal.[74]

[71] Ibídem., p. 101.
[72] Ibídem., p. 102.
[73] Ídem.
[74] Ídem.

CAPITULO SEGUNDO

LA CONSTRUCCIÓN DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS EN EUROPA

SUMARIO: INTRODUCCIÓN. 1. JURISPRUDENCIA DEL TRIBUNAL CONSTITUCIONAL FEDERAL DE ALEMANIA. 1.1. Sentencia del Tribunal Constitucional Federal Alemán, de 15/12/1983, que declara inconstitucional algunos preceptos de la Ley del Censo. 1.2. Sentencia del Tribunal Constitucional Federal Alemán, de 27/02/2008, sobre confidencialidad e integridad de los sistemas tecnológicos y de información. 2. EL PROCESO DE CONSTRUCCIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS EN ITALIA. 2.1 Recepción integral de la *privacy* norteamericana. 2.2. El derecho a la *riservatezza*. 2.3. La libertad informática. 3. LA CONSTRUCCIÓN DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS EN ESPAÑA. 3.1. El aporte desde la doctrina a la construcción de este derecho. 3.2. Jurisprudencia del Tribunal Constitucional español.

INTRODUCCIÓN

En el presente capítulo, analizo brevemente el origen y desarrollo del derecho fundamental a la protección de la protección de datos de carácter personal en tres países de la Unión Europa: Alemania, Italia y España. Su elección, se debe a que en todos ellos se ha producido un desarrollo legislativo, dogmático y jurisprudencial que les ha permitido, a lo largo de los últimos treinta años, configurar la protección de los datos de carácter personal como un nuevo derecho fundamental. Este proceso actualmente es mirado con atención desde Latinoamérica en general, y desde Chile en particular. Si se consultan la incipiente legislación especial que se ha dictado en los últimos años en los países de nuestro entorno destinado a cautelar los datos de carácter personal, es evidente la influencia de la experiencia europea en la materia.

Los tres países europeos elegidos, representan diversas formas de cómo se ha abordado la incorporación de este nuevo derecho al conjunto de derechos fundamentales. Tanto Italia como Alemania, sus Constituciones no tienen un precepto que recoja de manera expresa la protección del ciudadano frente a la informática. En

cuanto a España, si bien la Constitución de 1978 posee una referencia expresa a la limitación del uso de la informática (artículo 18.4), debieron pasar más de veinte años para que el Tribunal Constitucional reconociera este nuevo derecho fundamental de forma autónoma e independiente al derecho a la intimidad.

Si bien los tres países han abordado el tema de formas distintas, los argumentos construidos para la defensa de este nuevo derecho constitucional poseen elementos comunes, que es necesario desatacar. Ello nos permitirá tener claro cuáles son los presupuestos conceptuales sobre los cuales se articula la construcción del derecho a la autodeterminación informativa o protección de datos personales.

Cabe advertir que el enfoque de este apartado está puesto en la forma cómo la doctrina, jurisprudencia y legislación europea han interactuado e intentado dar respuesta a los fenómenos disfuncionales que el uso de la informática y las tecnologías de la información y comunicación (en adelante, TIC) han provocado en la sociedad europea. Frente a esta realidad, surge la necesidad de dar una cobertura legal y constitucional a las personas frente a los peligros que significaba el uso cada vez más extendido de las TIC, tanto en el ámbito público como privado. Las propuestas han sido variadas.

Así, encontramos algunas que propugnaban una recepción amplia de la *privacy* norteamericana, tanto en su denominación como en su contenido; otras que pretendían establecer un cierto paralelismo entre la *privacy* y el derecho a la intimidad, vida privada o *riservatezza*, tratado de ampliar el contenido de estas a fin de dar cobertura a la nueva realidad que se presentaba;[75] y aquellas que proponen la construcción de un nuevo derecho fundamental con identidad propia, a fin de tutelar adecuadamente a las personas frente a los peligros generados por parte de la informática y las TIC.

Adelantando en parte las conclusiones, cabe señalar que esta última opción, será la que terminará imponiéndose, al ser reconocido el derecho a la protección de datos personales como un derecho fundamental autónomo e independiente de otros derechos fundamentales, tanto en el artículo 8º de la Carta de Derechos Fundamentales de la

[75] En el mismo sentido véase Mª Mercedes SERRANO PÉREZ, *El derecho fundamental a la protección de datos…,* op. cit., p. 34

Unión Europea (CDFUE), como en la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH).

Ahora revisaremos brevemente el proceso de construcción de este derecho fundamental en cada uno de estos tres países mencionados, a objeto de establecer los elementos que llevaron al desarrollo de este nuevo derecho, su finalidad, contenido esencial, características, así como sus límites y garantías necesarias para su respeto.

1. JURISPRUDENCIA DEL TRIBUNAL CONSTITUCIONAL FEDERAL DE ALEMANIA

La tutela de los individuos frente a la informática fue abordada por la doctrina y jurisprudencia alemana de un modo original. No intentaron incorporar el concepto de *privacy* norteamericano, ni se generó la discusión en torno al concepto de intimidad o vida privada, como en otros países de Europa. El fundamento de dicha protección en el caso alemán se centró en el terreno del derecho al libre desarrollo de la personalidad y del respeto a la dignidad humana. De estos derechos, se extrajeron los presupuestos para la construcción del derecho a la autodeterminación informativa.

La jurisprudencia del Tribunal Constitucional Federal de Alemania (en adelante. TCFA) sobre la materia, ha sido esencial en este proceso. En particular, dos sentencias del TCFA han sido claves en la materia. Una, que declaró inconstitucional algunos preceptos de la Ley del Censo de 1983, estableciendo los elementos esenciales que configuran el derecho a la autodeterminación informativa y otra más reciente, de 2008, que establece los alcances de dicho derecho en relación con la integridad y confidencialidad de los nuevos sistemas tecnológicos de información y comunicación.

1.1. Sentencia del Tribunal Constitucional Federal Alemán, de 15/12/1983, que declara inconstitucional algunos preceptos de la Ley del Censo

La consagración de este nuevo derecho a la autodeterminación informativa se produce en la célebre Sentencia del TCFA[76], de 15 de diciembre de 1983, que declara inconstitucional algunos preceptos de la Ley del Censo, de 31 de marzo de 1982.[77]

Ésta Ley imponía a los ciudadanos la obligación de responder un detallado cuestionario con preguntas sobre distintos ámbitos de su vida personal, bajo la amenaza de una fuerte sanción pecuniaria en caso de negarse a responder.[78] En contra dicha Ley se interpuso un recurso de amparo constitucional, fundado en que diversos preceptos de la Ley del Censo violaban los derechos al libre desenvolvimiento de la personalidad y a la dignidad humana, a la libertad de expresión, y planteaba problemas en sus garantías procesales, derechos consagrados en los artículos 1, 2, 5 y 19, de la Ley Fundamental de Bonn.[79]

---

[76] La sentencia ha sido traducida al castellano, con un breve comentario introductorio, por Manuel DARANAS, en el *Boletín de Jurisprudencia Constitucional (BJC)*, nº 33, de 1984, pp. 126-170. Para un análisis crítico de la sentencia, véase Manuel HEREDERO HIGUERAS, «La Sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del Censo de la Población de 1983», *Documentación Administrativa*, nº 198, 1983, pp. 139-158; Ricard MARTÍNEZ MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa*, Madrid, Ed. Civitas, 2004, pp. 237-244; José Luis PIÑAR MAÑAS, "Protección de datos: origen, situación actual y retos de futuro", en *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, pp. 98 y ss.

[77] La Ley sobre el recuento de la población, de las profesiones, de las viviendas y de los centros de trabajo (Ley del Censo de 1983) de 25 de marzo de 1982, fue aprobada por el *Bundestag* el 4 de marzo de 1982 y publicada en el Boletín de Legislación Federal con fecha 31.3.1982, p. 369.

[78] A cada ciudadano se pedía responder detalladamente un cuestionario que podía llegar hasta 160 preguntas, entre las que figuraban el nombre, apellidos, dirección, teléfono, sexo, fecha de nacimiento, estado civil, pertenencia a alguna confesión religiosa, nacionalidad, convivencia con otros, sucesivos domicilios, actividad profesional, clase de ingresos, profesión aprendida, duración de la formación profesional, fin de los estudios medios, estudios universitarios, dirección del lugar de estudio o trabajo, medios de comunicación utilizados, tiempo empleado diariamente en desplazamientos, jornada laboral, clase, extensión, dotación y usos de la vivienda, número y uso de las habitaciones, cuantía de los alquileres mensuales, etc… Para ver el listado completo de los datos solicitados, véase los artículos 2, 3 y 4 de la Ley del Censo, reproducidos en Manuel DARANAS, en el *Boletín de Jurisprudencia Constitucional…,* op. cit., pp. 129-130.

[79] Llama la atención que al momento de dictarse la señalada Ley del Censo, Alemania contaba con una legislación especializada en materia de protección de datos, la *datenschutz* de 1977. La razón por la cual se tuvo que recurrir a la Constitución para realizar una defensa adecuada de los derechos afectados, fueron las deficiencias de la citada ley. Ante una regulación legal deficitaria, se optó por volver a la Constitución, esperando encontrar en ella la fuente adecuada para protegerse frente a los bancos de datos. Al respecto, SERRANO PÉREZ, señala que ello se explicaría, porque hasta antes de la elaboración del Censo de 1982, se había confiado en la "autosuficiencia legislativa" de dicha ley, si bien ya se habían denunciado los límites y lagunas de esta norma. Cfr. *El derecho fundamental a la protección de datos…,* op. cit., p. 63.

Es importante destacar el cambio de criterio en el TCFA que implicó la Sentencia contra la Ley del Censo. Antes de elaborar el concepto de autodeterminación informativa, el TCFA había recurrido a la llamada «teoría de la esferas» para tutelar los espacios más reservados de la persona, incluida la protección de la intimidad. Esta teoría distingue tres ámbitos de protección: la esfera privada, la *privatsphäre*, que se identifica con la noción de íntimo y protege el ámbito de la vida personal y familiar que se reserva del conocimiento de los demás; la *intimsphäre*, relacionada con la esfera de lo íntimo, secreto, cuya violación se produce cuando se conocen hechos o noticias que no se desea revelar; y la *individualphäre*, referido a todo aquello que atañe a la peculiaridad o individualización de una persona, como el honor, la imagen, el nombre. Estos diferentes ámbitos de la personalidad eran objeto de protección constitucional, de forma graduada, dependiendo de la esfera en la que se ubicaba el comportamiento del individuo.[80]

La teoría de las esferas, si bien sirve como forma de proteger la intimidad, presenta ciertas limitaciones en cuanto a la tutela de la vida privada frente al fenómeno de los bancos de datos personales.[81] Por ello el Tribunal buscó un nuevo fundamento jurídico específico no existente hasta ese momento en el ordenamiento alemán. De esta forma se crean dos construcciones paralelas y complementarias entre sí, que pertenecen al bloque de la protección de la personalidad, tronco común del cual ambas son extraídas. [82]

El TCFA construye su argumentación sobre la base del derecho general de la personalidad. Partiendo del artículo 2º, párrafo 1, en relación con el artículo 1º párrafo 1, de la Ley Fundamental, el Tribunal declaró que en «la clave de bóveda del ordenamiento de la Ley Fundamental se encuentra el valor y la dignidad de la persona, que actúa con libre autodeterminación como miembro de una sociedad libre», y a cuya

[80] Sobre el punto, véase Antonio Enrique PÉREZ LUÑO, *Derechos Humanos, Estado de Derecho y Constitución*, Tecnos, 10ª edición, Madrid, 2010, p. 334 y Mª Mercedes SERRANO PÉREZ, *El derecho fundamental a la protección de datos…,* op. cit., pp. 63 y 64.

[81] Al respecto, Manuel HEREDERO HIGUERAS, señala que el argumento de la vida privada se encuentra limitado para abarcar la nueva dimensión porque las cuestiones suscitadas en la sentencia «van desde la defensa de la intimidad y de la identidad hasta problemas de técnica legislativa». Cfr. «La sentencia del Tribunal Constitucional…», op. cit., p. 142.

[82] Carlos RUIZ MIGUEL, opina que Tribunal construyó el concepto de la autodeterminación informativa «ante la ausencia de expresa consagración en la GG de un derecho a la intimidad». Cfr. *La configuración constitucioncional del derecho a la intimidad*, Tecnos, Madrid, 1995, p. 95. En contra, véase SERRANO PÉREZ, *El derecho fundamental a la protección de datos…,* op. cit., p. 65.

protección se encamina este derecho de la personalidad. Agrega que, precisamente por influjo de la «evolución moderna y de las nuevas amenazas que lleva aparejadas para la personalidad cobra [el derecho a la autodeterminación informativa] significación especial».[83]

Por tanto, será el derecho general de la personalidad la sede para derivar el derecho matriz a partir del cual se elabora el derecho fundamental a la autodeterminación informativa (*informationelle Selbstestimmung)*, que tiene como misión preservar la identidad del individuo. El derecho a la libre personalidad, había sido configurado por la jurisprudencia del TCFA, como la libertad general de acción, que se concreta en la libertad para decidir la realización de determinados actos. De esta forma, la autodeterminación informativa queda configurada como la libertad de la persona para determinar quién, qué y con qué motivos puede conocer datos relativos al ella.[84]

Así, tenemos que el derecho general de la personalidad comporta la atribución al individuo de la capacidad de decidir, en el ejercicio de su autodeterminación, qué extremos desea revelar de su propia vida. Esta libertad de decisión, de control, supone además que el individuo tanga la posibilidad de acceder a su datos personales, que pueda, no sólo tener conocimiento de que otros procesan informaciones relativas a su

[83] Cfr. Considerando C. II de la Sentencia del TCFA. Respecto de la relación entre los derechos contenidos en estos dos preceptos de la constitución alemana, BENDA, señala que "el artículo 1.1 LFB contempla al individuo estáticamente «tal cual es», y el artículo 2.1 «tal cual actúa». Según este autor, este último artículo «contiene la idea esencial del artículo 1.1 GG como motivo y núcleo: la garantía del libre desarrollo de la personalidad responde en última instancia a la dignidad de la persona. Dado que la libertad no puede ser ilimitada, resultan posible las barreras previstas en el artículo 2.1 GG. No deberán, sin embargo ir más allá de donde lo permita *el contenido de dignidad humana* de la norma. Precisamente, los fundamentos contenidos en el artículo 2.1 GG no permiten que se vea afectada la esfera medular de la libertad personal». Cfr. Ernest BENDA, E., «Dignidad humana y derechos de la personalidad», en VV AA: *Manual de Derecho Constitucional* (Traducción de Antonio López Pina), Instituto Vasco de Administración Pública y Marcial Pons ed., Madrid, 1996, p. 123. Citado por Ricard Martínez, *Una aproximación crítica…,* op. cit., p. 239.

[84] Mª Mercedes SERRANO PÉREZ, *El derecho fundamental a la protección de datos…,* op. cit., p. 66. Al respecto el profesor DÍAZ REVORIO, identifica en este precepto la norma general de libertad que permite al Tribunal Constitucional Alemán introducir nuevos derechos fundamentales en el sistema, agregando que «se trata de "un derecho fundamental residual", lo suficientemente amplio para incluir cualquier manifestación de la libertad, desde los derechos a la vida privada y de la personalidad, hasta manifestaciones mucho menos trascendentes, como podría ser la libertad de dar de comer a las palomas» Cfr. DIAZ REVORIO, F. J., «Tribunal Constitucional y creación de derechos "no escritos"», en ESPÍN TEMPLADO, E. y DÍAZ REVORIO, F. J., (Coords.): *La justicia constitucional en el estado democrático*, Tirant lo Blanch, Valencia, 2000, p. 241.

persona, sino también someter el uso de éstas a un control, ya que, de lo contrario, se limitaría su libertad de decidir por autodeterminación.[85]

Como señala la sentencia, «no es posible la compatibilidad de un orden social y del ordenamiento jurídico que lo sostiene si el individuo no puede conocer quién, cuándo y con qué motivo cataloga, utiliza o transmite la información personal que le pertenece». La consecuencia de este razonamiento del tribunal, es el reconocimiento jurisprudencial de un derecho fundamental a la autodeterminación informativa basado en el derecho general de la personalidad, y que ofrece protección frente a la recogida, el almacenamiento, la utilización, y la transmisión ilimitada de los datos de carácter personal y «garantiza la facultad del individuo de decidir básicamente por sí sólo sobre la difusión y la utilización de sus datos personales».[86]

Al respecto, la sentencia señala:

> «…la autodeterminación del individuo presupone —también en las condiciones de las técnicas modernas de transmisión de datos— que se conceda al individuo la libertad de decisión sobre las acciones que vaya a realizar o, en su caso, a omitir, incluyendo la posibilidad de obrar de hecho en forma consecuente con la decisión adoptada. El que no pueda percibir con seguridad suficiente qué informaciones relativas a él son conocidas en determinados sectores de su entorno social y quien de alguna manera no sea capaz de aquilatar lo que puede saber de él sus posibles comunicantes puede verse sustancialmente cohibido en su libertad de planificar o decidir por autodeterminación. No serían compatibles con el derecho a la autodeterminación informativa un orden social y un orden jurídico que hiciese posible al primero, en el que el ciudadano ya no pudiera saber quién, qué, cuándo y con qué motivo sabe algo sobre él. Quién se siente inseguro de sí mismo en todo momento se registran cualesquiera comportamientos divergentes y se catalogan, utilizan o transmiten permanentemente a título de información procurará no llamar la atención con ese tipo de comportamiento» (Considerando C II a) de la Sentencia del TCFA).

El tribunal grafica lo anterior con el siguiente ejemplo:

> «Quien sepa de antemano que su participación, por ejemplo, en una reunión o en una iniciativa cívica va a ser registrada por las autoridades y que podrán derivarse riesgos para él por este motivo renunciará presumiblemente a lo que supone un ejercicio de los correspondientes derechos

[85] Ricard MARTÍNEZ MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa*, p. 240.
[86] Sobre el significado de la autodeterminación informativa en la Constitución alemana, véase el trabajo de A.E., PÉREZ LUÑO, «Libertad informática y derecho a la autodeterminación informativa», en I *Congreso sobre Derecho Informático*, Facultad de Derecho de la Universidad de Zaragoza, 1989, pp. 359-375.

fundamentales. Esto no sólo menoscabaría las oportunidades de desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición elemental de funcionamiento de toda la comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos» (Considerando C II a) de la Sentencia del TCFA).

De esta forma, el Tribunal deduce que:

«… la libre eclosión de la personalidad presupone en las condiciones moderna de la elaboración de datos la protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitadas de los datos concernientes a la persona. Esta protección cae, por tanto, dentro del ámbito del derecho fundamental del art. 2, párrafo 1, en relación con el artículo 1, párrafo 1, de la Ley Fundamental. El derecho fundamental garantiza, en efecto, la facultad del individuo de decidir básicamente por sí solo sobre la difusión y utilización de sus datos personales» (Considerando C II a) de la Sentencia del TCFA).

Estaríamos en presencia de un derecho fundamental que garantiza:

«… la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por él mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida» (Considerando C II a) de la Sentencia del TCFA).[87]

Teniendo en cuenta los elementos mencionados, la autodeterminación informativa se ha definido «como el derecho del individuo a controlar la obtención, tenencia, tratamiento y transmisión de datos relativos a su persona, decidiendo en cuanto a los mismos, las condiciones en que dichas operaciones pueden llevarse a cabo».[88] Como se puede apreciar, la atención se centra en el control de la utilización de la información personal, no en su calificativo de íntimo, reservado, secreto o privado, por lo que no es significativa su mayor o menor proximidad al núcleo íntimo de la persona, «razón por la cual la teoría de las esferas no ofrecía una argumentación adecuada».[89]

[87] Manuel DARANAS, *BCJ*, op. cit., p. 153.
[88] Mª Mercedes SERRANO PÉREZ, *El derecho fundamental a la protección de datos…,* op. cit., p. 67.
[89] Ibídem, pp. 67-68. Al respecto, Manuel HEREDERO, señala que lo grave «es la perdida de dominio de la información personal por parte de los interesados. La posibilidad de una interconexión de los sistemas de información o de un intercambio de datos entre distintos entes u órganos de la Administración implica que los datos personales pasan a formar parte de los grandes sistemas de información, sin que el interesado pueda saber dónde figura su propia información y, lo que es más grave aún, al perderse el rastro de su información como consecuencia de tales intercambios de la misma entre órganos o entes diversos y de su entrada en los sistemas de información, el derecho de acceso reconocido en la legislación de protección de datos resulta letra muerta». Manuel HEREDERO HIGUERAS, «La sentencia…», op. cit., p. 144.

En cuanto a la naturaleza jurídica del derecho a la autodeterminación informativa, se han planteado dos posturas: las que lo ven como un nuevo derecho fundamental autónomo, y las que le niegan tal carácter. Entre los primeros, se encuentra el Profesor Antonio Pérez Luño, para quién «negar la autonomía del derecho a la autodeterminación informativa, para englobarlo en el derecho al libre desarrollo de la personalidad, dificultaría la relación directa de aquél con otros derechos fundamentales». Agrega que «para garantizar la libertad informática —equiparada a la autodeterminación informativa— conviene, por tanto, concebirla como un derecho fundamental autónomo dotado de medios específicos de tutela. Por el contrario, disuelta en el ámbito de otros valores o derechos la autodeterminación informativa, corre el riesgo de relativizarse y ver comprometida su efectiva realización»[90]

Entre los autores que no consideran la autodeterminación informativa como un nuevo derecho fundamental destaca Erhard Denninger, para quién ni la denominación de autodeterminación informativa es nueva, ni es creación del Tribunal Federal, ni representa el nacimiento de un nuevo derecho fundamental con un objeto nuevo. En lo que atañe al objeto, porque se trata del resultado de una larga evolución jurisprudencial dirigida al reconocimiento y elaboración del derecho general de la personalidad; y en lo tocante a la terminología porque esta expresión había sido utilizada por la doctrina jurídica alemana a partir del año 1971.[91]

Otra crítica al establecimiento de la autodeterminación informativa como derecho fundamental autónomo, se ha realizado por quienes ven en esta proclamación una especie de derecho de propiedad sobre los datos, con el peligro que deriva de una concepción privatista semejante, en el sentido de erigirnos como dueños absolutos de nuestros datos.[92] En esta misma línea, Spiros Simitis critica la propuesta de modificar la constitución alemana para incluir un derecho a la protección de datos de forma expresa.[93]

---

[90] Antonio Enrique PÉREZ LUÑO, «El derecho a la autodeterminación informativa…», op. cit., p. 326 y 329.
[91] Erhard DENNINGER, «El derecho a la autodeterminación informativa», *Problemas actuales de la documentación y la informática jurídica*, Tecnos, 1987, p. 273. Citado por SERRANO PÉREZ, op. cit., p. 69.
[92] Cfr. SERRANO PÉREZ, *El derecho fundamental…,* op. cit., p. 69.
[93] Ídem.

Esta inquietud, acerca de la conversión del derecho a la autodeterminación informativa como un derecho patrimonialista e individualista, es compartida por Pérez Luño, pero éste último discrepa en cuanto a que para evitar dicha situación se deba sacrificar la autonomía de la autodeterminación informativa como derecho fundamental, para quedar relegada al mero apéndice de otros valores o derechos básicos.[94] También Serrano, es de la opinión de que la crítica formulada por Simitis no es válida, porque «la sentencia no atribuye al sujeto un ilimitado dominio sobre las informaciones. Al contrario, el Tribunal establece restricciones necesarias para preservar los intereses generales», por lo que a su juicio, éste peligro de apropiación exclusiva de datos no constituye una amenaza.[95]

En cuanto a los límites del derecho a la autodeterminación informativa, la propia sentencia se encarga de señalar que este derecho no se configura como un derecho absoluto, ya que encuentras sus limitaciones en la propia carta fundamental. Expresamente señala:

> «b) Este derecho a la "autodeterminación informativa" no está, sin embargo, garantizado sin límites. El individuo no tiene ningún derecho sobre "sus" datos en el sentido de una soberanía absoluta e irrestringible, sino que, es más bien una personalidad que se desenvuelve dentro de una comunidad social y que está llamada a comunicarse […]. La Ley Fundamental ha resuelto la tensión individuo-comunidad en el sentido de la referencia y la vinculación comunitarias de la persona, como ya se ha puesto varias veces de relieve en la jurisprudencia del Tribunal Federal […] El individuo tiene, pues, que aceptar en principio determinadas limitaciones de su derecho a la autodeterminación informativa en aras del interés preponderante de la colectividad» (Considerando C II b) de la Sentencia del TCFA).[96]

Por tanto, la autodeterminación informativa no es un derecho ilimitado. De acuerdo a la sentencia se podría limitar este derecho cuando exista un interés preeminente de la sociedad. Para ello se requiere un fundamento legal que responda al imperativo de claridad normativa y al principio de proporcionalidad, y la adopción de garantías organizativas y jurídico-procesales que aseguren suficientemente los derechos del ciudadano.[97]

---

[94] Cfr. Enrique Antonio, PÉREZ LUÑO, «El derecho a la autodeterminación informativa…», op. cit., p. 324.
[95] Cfr. SERRANO PÉREZ, *El derecho fundamental…,* op. cit., p. 69 y 70.
[96] Manuel DARANAS, *Boletín de Jurisprudencia Constitucional*, op. cit., p. 154.
[97] En el mismo sentido véase Ricard MARTÍNEZ, *Una aproximación crítica…,* op. cit., p. 241 y SERRANO PÉREZ, *El derecho fundamental…,* op. cit., pp. 70 y 71.

Sintetizando los argumentos y razonamiento utilizados por el TCFA para consagrar el derecho a la autodeterminación informativa, podemos señalar:[98] El soporte jurídico positivo de la sentencia, son los artículos 1.1 y 2.1 de la Ley Fundamental de Bonn, que consagran la inviolabilidad de la dignidad del hombre y el derecho al libre desenvolvimiento de la personalidad.[99]

Los fundamentos de la sentencia del TCFA fueron **los valores de libertad y dignidad humana en relación con el desarrollo de la personalidad**.[100] En ningún caso es la intimidad el fundamento último de la resolución, entre otras razones porque no existe un reconocimiento positivo de tal derecho, el cual ha sido tutelado exactamente por el mismo procedimiento que la autodeterminación informativa, y, en lo esencial, con la misma fundamentación.[101]

Otro razonamiento que se deriva de la sentencia del TCFA, sería la idea de **autodeterminación** en el sentido de autonomía individual, de libertad de decidir, por acción o por omisión, sobre las propias acciones sin injerencias externas. El tratamiento automatizado de los datos de carácter personal puede repercutir en esa libertad de decidir en la medida en que el individuo no sabe lo que los terceros conocen de él y en cuanto siendo conocedores de información de su persona, ellos sí puedan prever su decisión.[102]

En tercer lugar, de los argumentos esgrimidos por el TCFA se deduce con claridad que el tratamiento automatizado de datos personales puede repercutir no sólo sobre la

---

[98] En el desarrollo de esta síntesis seguimos a Ricard MARTÍNEZ, *Una aproximación crítica…,* op. cit., p. 241 y ss.

[99] «1.1 La dignidad del hombre es inviolable. Respetarla y protegerla es obligación de todo poder público»
«2.1 Todos tienen derecho al libre desenvolvimiento de su personalidad siempre que no vulnere los derechos de los otros ni atenten al orden constitucional o a la moral». Traducción tomada de: ÁLVARES VÉLIZ, Mª I. y ALCÓN YUSTAS, Mª F., *Las Constituciones de los Quince Estados de la Unión Europea: Textos y comentarios.* Dikynson, Madrid, 1996, p. 23. Existen otras traducciones de estos artículos de la Constitución alemana, como la contenida en el artículo de Manuel DARANAS en el *Boletín de Jurisprudencia Constitucional (BJC)*, op. cit., pp. 126-170.

[100] Para BENDA, la Sentencia de la Ley del Censo y la categoría de la autodeterminación informativa son «la concreción jurídica del derecho común de la personalidad, con la que se trata de combatir las amenazas a la personalidad producidos por los recientes cambios». Cfr. Ernst BENDA «Dignidad humana y derechos de la personalidad»…, op. cit., p. 132. Citado por Ricard MARTÍNEZ, *Una aproximación crítica…, op. cit.,* p. 241.

[101] Cfr. Ricard MARTÍNEZ, op. cit., pp. 241 y 242.

[102] Ibídem, p. 242.

libertad individual sino también sobre el **interés público**, en la medida en que libertad individual es un presupuesto básico de la convivencia democrática.[103]

La sentencia del TCFA abre una nueva vía para la tutela de los derechos fundamentales frente a las repercusiones asociadas al uso de TIC. Pero como hemos visto no existe unanimidad en la doctrina para señalar que dicha tutela constituye el nacimiento de una categoría nueva y autónoma de derecho.[104]

Por último, es interesante la opinión de Benda, quién sitúa el conflicto en otro plano, señalando que «el peligro para la privacidad del individuo no radica en que se acumule información sobre él, sino más bien, en que se pierda la capacidad de disposición sobre ella y respecto a quién y con qué objeto se transmiten. La privacidad se destruye no por la información en sí misma, sino por su transmisión disfuncional sobre la que el afectado pierde toda posibilidad de influir». Es más, agrega que «el que las informaciones puedan considerarse *sensibles* no dependen de que afecten circunstancias íntimas. Bajo las condiciones actuales del tratamiento automático ningún dato es *insignificante*. La limitación legítima del derecho a la autodeterminación informativa dependerá de a qué fin se requieren los datos, y qué posibilidades de combinación existen. A partir de ahí, deja de ser decisivo que la información requerida pertenezca a un *reducto* de la personalidad absolutamente protegido o a una esfera con referencias sociales».[105]

Vista la Sentencia del TCFA de 1983, que declaró inconstitucional algunas disposiciones de la Ley del Censo, configurando el derecho a la autodeterminación informativa, pasamos a revisar otra importante sentencia dictada recientemente por el mismo Tribunal.

---

[103] Al respecto Ricard MARTÍNEZ señala que el concreto ejemplo de repercusión que sugería el Tribunal relativo a la libre participación en reuniones públicas induce a pensar que más allá del conflicto entre el proceso de datos y la intimidad existen otros derechos sobre los que las tecnologías de la información pueden repercutir. Cfr. op. cit., p. 242

[104] Al respecto Ricard MARTÍNEZ señala que «tampoco puede afirmarse con rotundidad que dote de autonomía a la nueva institución ya que ésta, al igual que el propio derecho a la vida privada, se inserta en el derecho general de la personalidad», *Una aproximación crítica…,* op. cit., p. 243.

[105] Ernst BENDA, «Dignidad humana y derechos de la personalidad»,…op. cit., pp. 131 y 132. Citada por Ricard MARTÍNEZ, op. cit., pp. 242 y 243.

1.2. Sentencia del Tribunal Constitucional Federal Alemán, de 27/02/2008, sobre confidencialidad e integridad de los sistemas tecnológicos y de información

El TCFA, dictó el 27 de febrero de 2008, otra importante Sentencia, que está llamada a constituirse también en un referente obligado sobre la materia, al reconocer, por primera vez, el derecho a la confidencialidad e integridad de los sistemas tecnológicos y de información.[106] Con ello, da un paso más en la concreción y actualización del derecho a la autodeterminación informativa, tomando en consideración los avances técnicos de los últimos años.

El origen del pronunciamiento del Tribunal, se encuentra en el recurso interpuesto contra la reforma de la Ley de los Servicios de Inteligencia del Estado de Renania del Norte Westfalia. Esta Ley permitía expresamente que tales servicios pudiesen utilizar de forma secreta un software troyano (*spywere)*[107] para espiar los ordenadores de cualquier sospechoso, captando todo tipo de información, que luego puede ser analizada.

El Tribunal declaró inconstitucional la reforma y configuró, por primera vez, lo que algunos autores consideran «un nuevo derecho fundamental a la protección de la confidencialidad e integridad de los sistemas tecnológicos de información».[108] Se señala que el Tribunal de Karlsruhe da así un paso más en el reconocimiento, primero, del derecho a la autodeterminación informativa (en 1983 como ya sabemos) y más tarde del derecho a la protección absoluta de la zona nuclear del comportamiento privado.[109]

---

[106] Cfr. 1 BvR 370/07 de 27.2.2008. Disponible online: <http://www.bverfg.de/en/search.html>

[107] Aplicaciones informáticas, que normalmente forman parte de programas gratuitos, que de manera inadvertida se dedican a monitorear el comportamiento del usuario en la Red y a transmitir los resultados. Cfr. Anexo II: Glosario, del libro de María del Carmen GUERRERO PICÓ, *El impacto de internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Thomson-Civitas, Navarra, 2006, p. 586.

[108] Cfr. José Luis PIÑAR MAÑAS, «Protección de datos: origen, situación actual y retos de futuro», en *El derecho a la autodeterminación informativa,* Fundación Coloquio Jurídico Europeo, Madrid, 2009, pp. 98 y ss.; *Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio*, Documento de trabajo 147/2009, Fundación Alternativas, pp. 10 y 11. Disponible online, en <https://encrypted.google.com/#hl=es&sugexp=gsihc&xhr=t&q=sentencia+del+tribunal+constitucional+aleman,+27/02/2008&cp=56&gs_gbg=r6dgUy8VYd&pf=p&sclient=psy&source=hp&aq=f&aqi=&aql=&oq=sentencia+del+tribunal+constitucional+aleman,+27/02/2008&pbx=1&bav=on.2,or.r_gc.r_pw.&fp=8711c4f8ce7e0dc2&biw=1280&bih=591> [fecha consulta: 20.7.2011]

[109] Ídem.

Al igual que la sentencia de 1983, el Tribunal razona sobre la base del respeto del derecho al libre desarrollo de la personalidad, al señalar:

> «De la relevancia del uso de los sistemas tecnológicos de información para expresar la personalidad y de los peligros que para la personalidad representa tal uso, deriva una necesidad de protección que es significativa para los derechos fundamentales. El individuo depende de que el Estado respete las expectativas justificables de confidencialidad e integridad de tales sistemas de cara a la irrestricta expresión de su personalidad» (Epígrafe 181 de la Sentencia).

> «Los sistemas de información protegidos por este nuevo derecho son todos aquellos (ordenadores personales, PDAs, teléfonos móviles…) que solos o interconectados con otros pueden contener datos personales del afectado de modo que el acceso al sistema permite hacerse una idea sobre aspectos relevantes del comportamiento vital de una persona o incluso obtener una imagen representativa de su personalidad» (Epígrafe 203 de la Sentencia).

En cuanto a los límites a este nuevo derecho a la integridad y confidencialidad de los sistemas tecnológicos de información, al tener la consideración de un verdadero derecho constitucional, sólo puede ser restringido en casos muy limitados. Así, los poderes públicos del Estado pueden hacer uso de técnicas de registro online, en caso de peligro concreto para la vida, la integridad física o la libertad de las personas, así como para los fundamentos del Estado.

En consecuencia, dicha técnica no puede ser utilizada en las investigaciones relacionadas con delitos comunes ni en la actividad genérica de los servicios de inteligencia. Y que en cualquier caso «requieren la adopción de medidas para proteger el núcleo central de la vida privada (*core area of private conduct of life)*, que incluye la información relativa a las relaciones y los sentimientos personales».[110] Por ello, «el Tribunal señala que en casos de que de forma accidental se recabasen datos referidos a esa área vital, deben ser suprimidos de inmediato sin que puedan ser utilizados en ningún caso».[111]

Para concluir, queremos destacar la labor realizada por el TCFA, primero como precursor del derecho a la autodeterminación informativa en Europa, y luego, como defensor del mismo ante las nuevas aplicaciones tecnologías. Como destaca Piñar, con esta última sentencia «el derecho a la privacidad alcanza también a los dispositivos

[110] José Luis PIÑAR MAÑAS, «Protección de datos:…», op. cit., p. 100 y 101.
[111] Ídem.

informáticos que utilizamos y que forman parte ya de nuestra propia vida», los cuales contienen información que nos identifica y que puede dar una imagen o perfil certero de nuestra personalidad.[112] De esta forma el derecho a la protección de datos avanza en su desarrollo y actualización, adecuándose a las nuevas necesidades de los ciudadanos en la era tecnológica.

2. EL PROCESO DE CONSTRUCCIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS EN ITALIA

Este proceso tiene ciertas particularidades que llaman la atención. De partida, al igual que el caso alemán, la Constitución Italiana carece de un precepto que recoja la protección del individuo frente a la informática, lo que es lógico, en atención al tiempo en cual fue elaborada.[113] Producto de esta situación, se suscitó el problema del encuadre constitucional de este nuevo derecho, surgiendo distintas posturas en la doctrina italiana que tienen como elemento común buscar fórmulas para realizar una adecuada defensa de los derechos de las personas frente a los riesgos potenciales del uso de la informática.

Mirado desde un punto de vista evolutivo, se pueden distinguir las siguientes tendencias o corrientes en la doctrina italiana. En primer lugar, estarían los autores que hablan del derecho a la *privacy* o han intentado una traducción aproximativa del mismo.[114] Luego, estarían los partidarios de la *riservatezza*, en sentido amplio, de modo que comprenda la protección de datos personales. Por último, están quienes proponen construir una estructura o figura jurídica expresamente para la defensa de este nuevo derecho, que reúna todas las novedades aportadas por este fenómeno, a la que denominan *libertad informática*.[115]

---

[112] Ibídem, p. 101.

[113] La Constitución de la República italiana, fue promulgado el 27 de diciembre de 1947 y entró vigor el 1 de enero de 1948.

[114] Para Mª Mercedes SERRANO PÉREZ, estos autores, en realidad, son defensores de un derecho a la «*riservatezza*», en sentido amplio. Cfr. *El derecho fundamental a la protección de datos*, op. cit., p. 35-36.

[115] Para el desarrollo de este apartado se han seguido preferentemente las obras de: Mª Mercedes SERRANO PÉREZ, *El derecho fundamental a la protección de datos*, op. cit., pp. 33-60; Vittorio FROSINI, «Banco de datos y tutela de la persona», *Revista de Estudios Políticos* (Nueva Época), nº 30, noviembre-diciembre, 1982, pp. 21-40; y Tommaso Edoardo FROSINI, «Nuevas tecnologías y constitucionalismo», *Revista de Estudios Políticos (Nueva Época)*, núm. 124, abril-junio, 2004, pp. 129-147.

2.1. La recepción integral de la *privacy* norteamericana

La propuesta de recepcionar la *privacy* norteamericana por parte de la doctrina italiana, se produce como consecuencia de la informatización de la sociedad. Ante los peligros que conlleva la acumulación y tratamiento de datos representaba y la falta de una previsión constitucional que proteja adecuadamente dicho derecho, se busca un concepto idóneo para la tutela de los mismos, volviendo la mirada hacía la *privacy* norteamericana.[116]

El vocablo *privacy* ha gozado de tal aceptación por parte de la doctrina italiana que ha desbancado en gran parte al término *riservatezza*.[117] Esta última palabra tendría un significado sinónimo al de intimidad o vida privada. Entre los autores italianos que proponen la utilización del término *privacy* sin ninguna alteración, se encuentran Martinotti, Alpa, Feri y Rodota.[118] A estos autores, les parece correcta su utilización, toda vez que ella da cuenta tanto de la defensa de cualquier aspecto de la vida privada —con carácter general—, como de la protección del individuo frente a la informática —con carácter singular—. Cabe hacer presente que una doctrina minoritaria, conscientes de la imposibilidad de acoger en forma inalterada el concepto de *privacy* americano en Italia, proponen traducciones que se acerquen lo más fiel posible al citado término, como sería la vocablo *privatezza*.[119]

Otro sector de la doctrina critica la utilización del término *privacy* en Italia. Señalan que ella «alude a una idea general, a un concepto abstracto, que como tal puede ser válido, pero no como derecho concreto, configurado con esa categoría en el ordenamiento italiano, esto es, como derecho susceptible de reivindicación por parte de los ciudadanos».[120] En la misma línea, Guido Martinotti señala que la lengua italiana carece de un término equivalente al americano, no solo desde el punto de vista terminológico sino también semántico, ya que «la *privacy* en versión americana agrupa

[116] Cfr. SERRANO PÉREZ, *El derecho fundamental…,* op. cit., p. 37 y 38.
[117] Ídem.
[118] Guido MARTINOTTI, «La difessa della "privacy" I», *Politica del diritto*, anno II, núm 6, diciembre, 1971, pp. 749-779; Guido ALPA, «Privacy e statuto dell'informazione», *Banche dati, telemática e diritti della persona*, Cedam, Padova, 1984, p. 201; Giovanni B. FERRI, «Privacy e libertà informatica» *Banche dati, telemática e diritti della persona*, Cedam, Padova, 1984, pp. 45 y ss.; Stefano RODOTA, «Privacy e costruzione della sfera privata. Ipotesi e prospettive», *Politica del diritto*, anno XXII, núm. 4, dic. 1991.
[119] Para un desarrollo de esta corriente doctrinaria, véase la bibliografía citada por SERRANO PÉREZ, *El derecho fundamental…*, op. cit., p.38, en los pie de página 22 y 23.
[120] Ibídem., p. 36.

una variedad y complejidad de contenidos que no son asimilables a ninguna figura existente en el idioma latino».[121] Por tanto, dicha recepción sería parcial, sólo referida a un aspecto de ella. Esta cubriría únicamente la protección de las personas frente a la informática, a diferencia de la *privacy* americana que se plantea como un "macroderecho", que incluye varios aspectos, los cuales, ya estarían cubiertos por otros derechos fundamentales en Italia.[122]

2.2. El derecho a la *riservatezza*

Una parte de la doctrina italiana intenta englobar la protección de los individuos ente los bancos de datos dentro del derecho a la *riservatezza*. Ésta ha sido definida como «el modo de ser de la persona que consiste en la exclusión de los otros del conocimiento de cuanto se refiere a la persona misma».[123] Se encuentra reconocido constitucionalmente, como protección de la persona frente a injerencias en su esfera física, centrado en el domicilio (artículo 14) y en el secreto de la correspondencia (artículo 15).[124] Este espacio de protección se amplía en algunas de sus manifestaciones a la libertad (artículo 13) y a la libre manifestación del pensamiento (artículo 21). La protección de situaciones no previstas en los artículos señalados, pero respecto de las cuales se necesita protección constitucional, se resuelven de acuerdo a esta teoría, mediante una interpretación amplia de los artículos 2 y 3 de la Constitución Italiana, que reconoce los derechos inviolables del hombre, necesarios para el desarrollo de su personalidad.[125] Con ello, se permitiría la inclusión de situaciones no previstas en el texto constitucional, que merezcan la calificación de derechos inviolables.

---

[121] Guido MARTINOTTI, «La difessa della "privacy"»…, op. cit., p. 751.
[122] Por todos, véase SERRANO PÉREZ, op. cit., p. 38.
[123] Guido ALPA, *Novissimo Digesto taliano*, vol. XVI, Torino, 1982, p. 115. Citado en SERRANO PÉREZ, *El derecho fundamental…,* op. cit., pp. 40-41.
[124] Art. 14. «El domicilio es inviolable: No se podrán efectuar inspecciones o registros ni embargos salvo en los casos y con las modalidades establecidas por la ley, y conforme a las garantías prescritas para la salvaguardia de la libertad personal. Se regularán por leyes especiales las comprobaciones e inspecciones por motivos de sanidad y de salubridad públicas o con fines económicos y fiscales.
Art. 15. Serán inviolables la libertad y el secreto de la correspondencia y de cualquier otra forma de comunicación. La limitación de los mismos sólo podrá producirse por auto motivado de la autoridad judicial con las garantías establecidas por la ley».
[125] Art. 2: «La República reconoce y garantiza los derechos inviolables del hombre, ora como individuo, ora en el seno de las formaciones sociales donde aquél desarrolla su personalidad, y exige el cumplimiento de los deberes inexcusables de solidaridad política, económica y social.
Art. 3: Todos los ciudadanos tendrán la misma dignidad social y serán iguales ante la ley, sin distinción de sexo, raza, lengua, religión, opiniones políticas ni circunstancias personales y sociales.

Esta doctrina postula que la referencia al art. 2 sobre los derechos inviolables del hombre es el fundamento común para los derechos que más adelante recoge expresamente la carta fundamental en los arts. 13 (la libertad); 14 (la inviolabilidad del domicilio); 15 (el secreto de las comunicaciones) y 21 (la libre manifestación del pensamiento). Pero también sirve para reconocer otras situaciones subjetivas, no contempladas expresamente en la Constitución, como derechos inviolables de la persona.

Así, dicho artículo cumpliría una doble función. Por una parte, serviría de fundamento común para las situaciones reguladas expresamente en la Constitución, y por otra, se constituiría en el fundamento constitucional ante la carencia de una norma expresa que regule y proteja nuevas situaciones que afecten derechos subjetivos inviolables de las personas y el desarrollo de su personalidad.[126] Para los autores que defienden esta teoría, esta figura sería la que más se aproxima a la *privacy* norteamericana.

Los críticos de la técnica de la *riservatezza* como forma de cautelar los datos personales, señalan que ella presentaría varias inconsistencias. Entre ellas, mencionan la inexistencia en Italia de un término de significado idéntico al de la *privacy* norteamericano, por la amplitud del contenido de ésta, la cual abarca una gran cantidad de situaciones. Así, la *riservatezza* no sería un instituto jurídico adecuado para encuadrar todas las necesidades derivadas de la protección de datos, por carecer aquella de una defensa jurídica en ese campo y, en general, en el de la elaboración electrónica datos personales.

Estos autores, sólo reconocen en la Constitución italiana manifestaciones concretas de la *riservatezza*, pero no lo reconocen como un derecho constitucional que proteja de forma global todas las facetas de la vida privada de las personas. Así, sólo el domicilio, las comunicaciones, en ciertos aspectos la libertad y el pensamiento serían

---

Constituye obligación de la República suprimir los obstáculos de orden económico y social que, limitando de hecho la libertad y la igualdad de los ciudadanos, impiden el pleno desarrollo de la persona humana y la participación efectiva de todos los trabajadores en la organización política, económica y social del país».

[126] Para un desarrollo del tema, véase Mª Mercedes SERRANO PÉREZ, *El derecho fundamental a la protección de datos…,* op. cit., pp. 39-55 y las obras citada por la autora.

derechos inviolables. Por tanto, el control sobre los datos personales, no estaría incluido dentro del ámbito de la *riservatezza*.[127]

Para ellos, no es sostenible en el ordenamiento constitucional italiano equiparar la *riservatezza* con la *privacy* norteamericana.[128] En este sentido Mirabelli, señala que aunque aceptáramos el enfoque más amplio posible de la *riservatezza*, no se solucionaría con ello todos los problemas, ya que se debe reconocer que «la tutela que el ordenamiento concede a ésta es una tutela represiva y sancionadora, que se pone en marcha al verificarse la lesión», mientras que «los intereses que se trata de proteger reclaman, por el contrario una tutela preventiva, dirigida a evitar la posibilidad misma de la lesión».

Por tanto, para estos autores, sería necesario construir una nueva posición jurídica, que considere todos los aspectos e intereses en juego.[129] En la misma línea, Frosini, señala que lo que se reconoce en estos artículos (13, 14, 15, 21) de la Constitución italiana, son distintas manifestaciones de situaciones que constitucionalmente tutelan ámbitos de reserva, pero, en definitiva, ámbitos muy concretos, sin que quepa derivar de ahí un derecho general al *riserbo*. Agrega que, falta en Italia un reconocimiento constitucional de un derecho a la *riservatezza* configurado de forma autónoma, como un derecho subjetivo a la intangibilidad de la esfera privada de la persona, lo que lo llevará a desarrollar su teoría sobre la libertad informática.[130]

Por último, otra parte de la doctrina italiana, haciéndose cargo de las críticas y con la finalidad de construir un concepto amplio de *riservatezza*, tanto en su aspecto negativo (freno a las injerencias por parte de terceros) como positivo

[127] Entre los autores que sustentarían esta teoría, se encuentran: Roberto TONIATTI, «Libertad informática y derecho a la protección de datos personales: principios de legislación comparada», en II Jornada de Estudio sobre la «protección de datos y derechos fundamentales», *Anuario de Jornadas, Servicio de Estudio del IVAP*, Oñati, 1991, p. 269, y Giuseppe MIRABELLI, «Le posizioni soggetive…», op. cit., p. 396 y ss. Citados en SERRANO PÉREZ, *El derecho fundamental…,* op. cit., p. 46 y 47.

[128] En la misma línea SERRANO PÉREZ, señala que es «es un error hablar indistintamente de la "*privacy*" y de la "*riservatezza*" queriendo identificar ambos términos», agregando que «no se pueden utilizar como sinónimos». Termina señalando que «puede que en algún punto de su contenido ambos términos se aproximen bastante, ya que ambas surgen para frenar injerencias no consentidas, pero la primera tiene una amplitud mayor que la segunda en cuanto a su ámbito de tutela», *El derecho fundamental…*, op. cit., p. 40.

[129] Mª Mercedes SERRANO, *El derecho fundamental…,* op. cit., p. 47.

[130] Vittorio FROSINI, «Banco de datos…», op. cit., p. 192. En mismo sentido SERRANO PÉREZ, *El derecho fundamental…,* op. cit., p. 41.

(autodeterminación informativa), recurren al art. 21 de la Constitución italiana.[131] Postulan que en dicho artículo se tutela también —junto a los arts. 2, 3, 13, 14 y 15— parte de la esfera reservada de la persona. Así, el art. 21 permitiría el control de la información por parte del individuo, otorgándole un cariz similar a la *privacy* norteamericana.[132] Serrano, critica esta postura porque recurre a aspectos fragmentarios de la *riservatezza*, lo que pone de manifiesto que no existe ningún precepto constitucional que permita elaborar una figura unitaria, descartando, por la misma razón, la posibilidad de una interpretación amplia de la misma.[133]

2.3. La libertad informática

La doctrina de la libertad informática nace en Italia a principio de los años ochenta con la intención de dar una respuesta teórica al problema que entonces preocupaba mayormente al jurista comprometido con la temática del derecho de la informática, que era el de la protección de la *riservatezza* con referencia a los bancos de datos.[134] Uno de sus principales exponentes, Vittorio Frosini, la define como «un derecho de autotutela de la propia identidad informática: o sea, el derecho de controlar (conocer, corregir, quitar o agregar) los datos personales inscritos en las tarjetas de un programa electrónico».[135]

---

[131] Art. 21: «Todos tendrán derecho a manifestar libremente su pensamiento de palabra, por escrito y por cualquier otro medio de difusión. Sólo se podrá proceder a la recogida por auto motivado de la autoridad judicial en el caso de delitos por los que lo autorice expresamente la ley de prensa o en el supuesto de violación de las normas que la ley misma establezca para la indicación de los responsables. En estos casos, cuando haya urgencia absoluta y no sea posible la intervención a tiempo de la autoridad judicial, podrá procederse a la recogida de la prensa periódica por funcionarios de la policía judicial, que deberán inmediatamente, y nunca más de veinticuatro horas después, ponerlo en conocimiento de la autoridad judicial. Si ésta no confirma la medida dentro de las veinticuatro horas siguientes se considera la recogida como nula y carente de efecto alguno. La ley podrá disponer, por preceptos de carácter general, que se den a conocer los medios de financiación de la prensa periódica. Se prohíben las publicaciones de prensa, los espectáculos y cualesquiera otras manifestaciones contrarias a las buenas costumbres. La ley establecerá medidas adecuadas para prevenir y reprimir las violaciones en este campo».

[132] En esta línea se encontraría Carlos CASONATO, quien en su trabajo, *Diritto alla*…, op. cit., pp. 105 y ss., analiza los pronunciamientos de la Corte Constitucional italiana sobre los artículos 2, 3, 13, 14 y 21 respecto de los distintos ámbitos de la «*riservatezza*».

[133] Mª Mercedes SERRANO PÉREZ, *El derecho fundamental…,* op. cit., p. 49.

[134] Tommaso Edoardo FROSINI, «Nuevas tecnologías y constitucionalismo», *Revista de Estudios Políticos (Nueva Época)*, núm. 124, abril-junio, 2004, p. 131.

[135] Vittorio FROSINI, «Bancos de datos y tutela de la persona», *Revista de Estudios Políticos* (Nueva Época), núm. 50, noviembre-diciembre 1982, p. 24; *Informática y Derecho*, Temis, Bogotá, 1988, p. 110; y «La protezione della riservatezza nella societá informática», op. cit., pp.37 y ss. En el mismo sentido, véase Stefano RODOTA, *Elaboratori elettronici e controllo sociale,* Il Mulino, Bolonia, 1973; 5-14; y

En su versión original, la libertad informática venía configurada en su vertiente positiva y negativa. La libertad informática negativa, expresa «el derecho a no difundir ciertas informaciones de carácter personal, privado, reservado» (calificativos estos, que podrían, en determinados casos, no coincidir entre ellos); en cambio, la libertad informática positiva expresa la facultad «de ejercitar un derecho de control sobre los datos concernientes a la propia persona que están fuera del marco de la *privacy* por haberse convertido en elementos de *input* de un programa electrónico, y por tanto, libertad informática positiva, o derecho subjetivo de reconocimiento, de conocimiento, de corrección, de recopilación o añadidura de datos en una tarjeta electrónica personal».[136]

Frosini, plantea que los aspectos positivos y negativos de este derecho, son complementarios entre sí, ya que «el ejercicio del derecho consiste precisamente en la facultad de intervenir sobre la composición de los datos, no sólo para limitar su uso, prohibiendo el acceso a otros, sino también para llevar a cabo una actividad de inspección que implique la verificación o cancelación que, por otra parte, se corresponde con el derecho de rectificación de la información por medio de la prensa o de la televisión».[137]

Sintetizando las diferentes posturas frente el fenómeno informático en Italia, se pueden señalar que, ante la inexistencia de un precepto constitucional expreso en la Constitución Italiana sobre la libertad informática, surgen diferentes argumentos desde la doctrina para dar cabida constitucional a esta libertad. Algunos autores, buscan su reconocimiento vinculándolo a derechos reconocidos constitucionalmente, tales como la libertad de información, la libertad de pensamiento, el secreto de las comunicaciones, etc.

Antonio Enrique PÉREZ LUÑO, «Informática y libertad», en *Revista de Estudios Políticos,* 1981, núm. 24, p. 31 y ss.

[136] Cfr. el informe de Vittorio FROSINI: «La protezione della riservatezza nella societá informática», en el vol. *Privacy e banche dei dati,* a cargo de N. MATERUCCI, Bologna, 1981, pp. 37 y ss. (después incluido en el vol. *id. Informática, diritto e societá,* 2.a ed., Milano, 1992, pp. 173 y ss.). Citado por Tommaso Edoardo FROSINI, «Nuevas tecnologías y constitucionalismo», op. cit., p. 131 y 132.

[137] Cfr. Vittorio FROSINI, «La protezione della», op. cit., p. 179.

Otra parte de la doctrina, plantea la necesidad de crear una nueva técnica inclusiva de todas las manifestaciones de este derecho. Recurren a los arts. 2 y 13 de la Constitución Italiana, para construir, desde la libertad personal, una visión completa y general del fenómeno informático. De esta forma, si la libertad informática es una garantía de la libertad del individuo y de todos los derechos fundamentales, abarcará en su protección la libertad de pensamiento, respetará el secreto de las comunicaciones y garantizará la libertad de información en sus vertientes de informar y también de ser informado.[138] De este modo, también, «el derecho de libertad informática asume una forma nueva del tradicional derecho de libertad personal, como derecho a controlar las informaciones sobre la propia persona, como derecho del *habeas data*».[139]

Respecto de la evolución jurisprudencial sobre la materia, Tommaso Frosini, señala que los Tribunales italianos han reconocido y afirmado este nuevo derecho de libertad en los términos de protección de la autonomía individual, como exigencia pasiva en relación con los detentadores del poder informático, de los particulares o de las autoridades públicas.[140]

En cuanto a la legislación italiana sobre protección de las personas respecto al tratamiento de datos personales —Ley núm. 675, de 1996—[141], al igual que muchos países de la comunidad europea, surge y se desarrolla por la necesidad de permitir a Italia entrar al espacio Schengen y cumplir con las obligaciones que se le imponían, tanto desde la Unión Europea con la Directiva 95/46/CE, como a nivel internacional, con la ratificación del Convenio núm. 108 de 1981 sobre la materia.[142]

Por último, cabe señalar que como consecuencia de la irrupción de Internet, el derecho a la libertad informática en Italia ha evolucionado, lo que permite mostrar su

[138] Cfr. Mª Mercedes SERRANO PÉREZ, *El derecho fundamental…,* op. cit., p. 49.
[139] Cfr. Tommaso Edoardo FROSINI, «Nuevas tecnologías y constitucionalismo», op. cit., p. 132.
[140] Ídem.
[141] Aprobada el 1 de diciembre de 1996. Cfr. Legge 675/96, *Gazzetta Ufficiale della Repubblica Italiana* n° 5, suplemento 3, 8.01.1997. Posteriormente el texto fue integrado y corregido en forma significativa por los Decretos Leyes nº 123, de 9.5.1997 y nº 255, de 28.7.1997.
[142] Sobre la legislación italiana en materia de protección de datos, véase Guido FRANCHI SCARSELLI, «Ley Italiana 675 de 1996 sobre privacidad informática», Revista Derecho del Estado, núm. 8, junio, 2000, pp. 31-43. Traducido por Santiago Perea Latorre, del artículo publicado originalmente en *Autonimie Locali e Servizi Sociali*, núm. 3, 1997, p. 505-515; Mario G. LOSANO, «La ley italiana sobre protección de datos personales», *Cuadernos constitucionales de la Cátedra Fadrique Furió Ceriol*, núm. 17, 1997, págs. 147-160.

actualidad teórica.[143] En efecto, señalan que con Internet el derecho de libertad informática «se ha transformado en una exigencia de libertad en sentido activo, no libertad "desde" sino libertad "de", que es la de valerse de los instrumentos informáticos para obtener información de todo género». Concebido de esta forma, este derecho permite y garantiza «la participación en la sociedad virtual, creada, generada, originada, con la llegada de los instrumentos electrónicos en la sociedad tecnológica: es una sociedad de componentes variables y de relaciones dinámicas, en la cual cada individúo participante es soberano en sus decisiones».[144]

Nos parece que esta postura, se centra exclusivamente en uno de los aspectos que pretende cubrir la libertad informática, la libertad de recibir y comunicar opiniones, información, etc., pero no constituye un aporte a la evolución de este derecho, sino más bien, una manifestación más de la estrecha relación que posee el derecho a la protección de datos con otros derechos fundamentales, como garante de los mismos.

3. LA CONSTRUCCIÓN DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS EN ESPAÑA

Atendido el objeto limitado de esta tesis, partiremos el estudio del desarrollo dogmático y jurisprudencial del derecho fundamental a la protección de datos personales en España desde la Constitución de 1978.[145] Para ello se revisará las

[143] Tommaso Edoardo FROSINI, «Nuevas tecnologías y constitucionalismo», op. cit., p. 132 y 133.

[144] Esta postura, plantea que «nos encontramos, indudablemente, frente a una nueva forma de libertad, que es la de comunicar con quien se quiere difundiendo opiniones propias, pensamientos propios y materiales propios, y la libertad de recibir. Por tanto, libertad de comunicar como libertad para transmitir y recibir. No es solamente el ejercicio de la libre manifestación de pensamiento del individuo , sino más bien la facultad de éste de constituir una relación de transmisión y solicitud de información, de poder disponer sin limitaciones del nuevo poder de conocimiento conferido por la telemática; en resumen, de poder ejercitar el derecho individual de libertad informática. Queda claro, pues, como en esta nueva concepción *tecnologizzata* de la libertad de comunicación resulta forzado sostener los contenidos de las libertades constitucionales tradicionales, en particular la de comunicación y la de manifestación de pensamiento. Por tanto, es la libertad informática la que representa la nueva libertad constitucional de la sociedad tecnológica, como demuestran algunas experiencias de Constituciones recientes y como puede recabarse, sin duda, a través de una interpretación evolutiva de las Constituciones menos recientes» Cfr. Tommaso Edoardo FROSINI, «Nuevas tecnologías y constitucionalismo», op. cit., p. 132 y 133.

[145] Para un estudio del nacimiento y desarrollo del derecho a la intimidad en España, existe una abundante bibliografía, entre otros véase Ricard MARTÍNEZ MARTÍNEZ, *Una aproximación crítica*, op. cit., pp. 61 y ss.; y Antonio Enrique PÉREZ LUÑO, «Informática y Libertad. Comentario al artículo 18.4 de la Constitución española», *Revista de Estudios Políticos* (Nueva Época), núm. 24, noviembre-diciembre, 1981, pp. 33 y ss.; C. RUIZ MIGUEL, *La Configuración Constitucional del Derecho a la Intimidad*, Tecnos, Madrid, 1995.

principales posiciones doctrinarias y la jurisprudencia más relevante del Tribunal Constitucional Español (en adelante, el TCE) en el proceso de elaboración de este nuevo derecho fundamental.

3.1. El aporte desde la doctrina a la construcción del derecho a la protección de datos

Al igual que el resto de los países europeos, la causa mediata del nacimiento de este nuevo derecho, la encontramos en la informatización de la sociedad y la creciente acumulación de información personal por parte de organismos públicos como por particulares.[146] Por ello, ha sido necesario el establecimiento de unas garantías que tutelen a los ciudadanos frente a la eventual erosión y asalto tecnológico de sus derechos y libertades. Como consecuencia del fenómeno social descrito, «este nuevo derecho del constitucionalismo democrático contemporáneo ha adquirido una creciente importancia, reconociéndose, por ejemplo en España, como derecho fundamental en el art. 18.4 de la Constitución Española (en adelante, indistintamente CE)».[147]

A diferencia de las Constituciones italiana y alemana, la Carta magna española hace una referencia expresa a la limitación del uso de la informática para garantizar el pleno ejercicio de los derechos de sus ciudadanos.[148] El artículo 18.4 de la Constitución Española, situado dentro de la sección derechos fundamentales y libertades públicas, señala: «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».

---

[146] Para un estudio sobre el desarrollo de la juscibernética y de la informática jurídica en España, véase Antonio Enrique PÉREZ LUÑO, *Derechos humanos, Estado de Derecho y Constitución*, Tecnos, 10ª edición, Madrid, 2010, pp. 378 y ss.y la bibliografía citada por el autor.

[147] Cfr. Mª Mercedes SERRANO PÉREZ, *El derecho fundamental a la protección de* datos, op. cit., p. 75. En el mismo sentido Antonio Enrique PÉREZ LUÑO, *Manual de Informática y Derecho*, Ariel, Barcelona, 1996, p. 45.

[148] Sobre la discusión generada en los diversos momentos del *iter* constituyente en el proceso de elaboración del apartado cuarto del artículo 18 de la Constitución española, véase Pablo LUCAS MURILLO DE LA CUEVA, *El derecho a la autodeterminación informativa*, Tecnos, Madrid, 1990, pp. 150-158. El mismo, autor, en una de sus últimas obras señala respecto de los motivos para integrar dicha disposición en el texto constitucional, que «para la mayoría de los constituyentes —salvo Miguel Roca Junyet, que propuso la redacción finalmente aprobada—, pesó más a la hora de aprobar el apartado cuarto del artículo 18 de la CE, la influencia de la Constitución portugués de 1976 y el deseo de incorporar las últimas novedades llegadas al constitucionalismo democrático que el convencimiento de su necesidad por tener una clara percepción de los peligros cuya amenaza pretende conjurar ese precepto». Cfr. «La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad», en *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europea, Madrid, 2009, p. 19.

Producto de la ambigüedad de su redacción, el debate doctrinal en España se centró sobre el bien jurídico protegido por el art. 18.4 de la CE. Algunos autores partiendo de una interpretación literal, plantearon el problema de la informática principalmente como una amenaza para la intimidad.[149]

Ante las insuficiencias y limitaciones propias de una interpretación extensiva del derecho a la intimidad para dar cabida a la protección frente al fenómeno informático, surge otra corriente doctrinaria, cuyo principal exponente es el Profesor de Derecho Constitucional y Magistrado del Tribunal Supremo, Pablo Lucas Murillo de la Cueva.[150] Este autor, plantea ignorar en parte el tenor literal del texto constitucional para darle una interpretación más idónea con los intereses que plantea el fenómeno tecnológico en general e informático en particular. Señala este autor, que el bien jurídico que el art. 18.4 protege es la libertad informática o —en fórmula menos estética pero más precisa— la autodeterminación informativa. Esta, «en cuanto posición jurídica subjetiva correspondiente al *status* de *habeas data*, pretende satisfacer la necesidad, sentida por las personas en las condiciones actuales de la vida social, de preservar su identidad controlando la revelación y el uso de los datos que les conciernen y protegiéndose frente a la ilimitada capacidad de archivarlos, relacionarnos y transmitirlos propia de la informática y de los peligros que esto supone».[151]

Este objetivo se consigue, según Lucas «por medio de lo que se denomina técnica de protección de datos, integrada por un conjunto de derechos subjetivos, deberes,

[149] En esta línea, véase Antonio Enrique PÉREZ LUÑO, «La protección de la intimidad frente a la informática en la Constitución española de 1978», *Revista de Estudios Políticos* (Nueva Época), núm. 9, mayo-junio 1979, pp. 73 y ss. Posteriormente, por todos, puede verse Antonio ORTI VALLEJO, *Derecho a la intimidad e informática*, Comares, Granada, 1994.

[150] Entre sus trabajos dedicados al tema de la protección de datos y la autodeterminación informativa, destacamos: *El derecho a la autodeterminación informativa*, Tecnos, Temas claves, Madrid, 1990; *Informática y protección de datos personales*, Centro de Estudios Constitucionales (CEC), Madrid, 1993; «Las vicisitudes del Derecho de la protección de datos personales», *Revista Vasca de Administración Pública*, núm. 58-II, 2000, pp. 211 y ss.; «La Constitución y el derecho a la autodeterminación informativa», *Cuadernos de Derecho Público*, núm. 19-20, 2003, pp. 27 y ss.; «Perspectivas del derecho a la autodeterminación informativa», en: «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas», *Revista de Internet, Derecho y Política*, UOC, núm. 5, 2007, [monográfico en línea] <http://www.uoc.edu/idp/5/dt/esp/lucas.pdf>; «La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad», en *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europea, Madrid, 2009, pp. 11-80.

[151] Cfr. Pablo LUCAS MURILLO DE LA CUEVA, *El derecho a la autodeterminación informativa*, op. cit., pp. 173-175

procedimientos, instituciones y reglas objetivas. El individuo que se beneficia de la misma adquiere así una situación que le permite definir la intensidad con que desea que se conozcan y circulen su identidad y circunstancias, combatir las inexactitudes o falsedades que las alteren y defenderse de cualquier utilización abusiva, desleal o, simplemente, ilegal que pretenda hacerse de las mismas».[152]

En su formulación original, esta doctrina planteaba la necesidad de otorgar poderes a su titular que le permitan definir los aspectos de su vida no públicos, que no desea que se conozcan, así como las facultades que le aseguren que los datos que de su persona manejan informáticamente terceros son exactos, completos y actuales y que se han obtenido de modo leal y lícito.[153] De este modo, el derecho a la autodeterminación informativa, se constituye en un poder de control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente, sea íntima o no, para preservar, de esta forma y en último extremo, la propia identidad, nuestra dignidad y libertad.

El ejercicio de la libertad por cada persona, es lo que se denomina «autodeterminación», que sumado al calificativo «informativa», indica definición o control por el afectado de la información que le concierne.[154] Esta elaboración, como hemos visto anteriormente, corresponde a la doctrina y jurisprudencia alemana, la que coincide básicamente con la libertad informática, en cuanto «busca garantizar a los ciudadanos unas facultades de información, acceso y control de los bancos de datos que les conciernen».[155]

Al igual que Italia, los términos utilizados para referirse al nuevo fenómeno jurídico vinculado a la protección de los derechos y libertades de las personas frente al

---

[152] Ídem.

[153] Pablo LUCAS MURILLO DE LA CUEVA, *Informática y Protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal)*, col 43 Cuadernos y Debates, CEC, Madrid, 1993, pp. 32 y 33. En el mismo sentido SERRANO PÉREZ, *El derecho fundamental…,* op. cit., p. 78.

[154] Cfr. Pablo LUCAS MURILLO DE LA CUEVA, «Perspectivas del derecho a la autodeterminación informativa». En: «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*, UOC, núm. 5, 2007, p. 20. Disponible en <http://www.uoc.edu/idp/5/dt/esp/lucas.pdf>.

[155] Cfr. Antonio Enrique PÉREZ LUÑO, «El derecho a la autodeterminación…», op. cit., p. 305. Lo vuelve a señalar en *Manual de Informática y Derecho*…, op. cit., p. 44.

uso de la informática han sido variados. Las principales denominaciones utilizadas por la doctrina y jurisprudencia española para referirse a este derecho son: intimidad informática, libertad informática, autodeterminación informativa y protección de datos personales.

Algunos autores plantean una distinción entre protección de datos personales y libertad informática. Señalan que ambos institutos, si bien aluden a la protección de este nuevo derecho fundamental, presentan un matiz diferenciador, relacionado con la función que cada uno de ellos cumple. Así, mientras la libertad informática es un derecho de las personas, la protección de datos, se refiere a la situación equilibrada de poderes que debería existir en los procesos de obtención, almacenamiento y transmisión de datos entre todos los sujetos implicados. La protección de datos, entonces, «vendría a ser el apoyo estructural, organizativo y objetivo de los archivos que contengan informaciones personales», y se dirigiría a establecer «normas de ordenación y de soporte físico de los mismos». Por su parte, la libertad informática o autodeterminación informativa, «se proyecta en mantener las garantías de las personas para mantener en equilibrio la situación de poder a que antes nos referíamos».[156] Ambas categorías se condicionan mutuamente y representan la misma realidad referida a la existencia de un nuevo derecho fundamental.[157]

En la actualidad la doctrina mayoritaria está de acuerdo en que la expresión protección de datos ha perdido su estricto sentido semántico para entender, incluida bajo esta denominación, la idea de protección de las personas, la cual se hallaría muy próxima a la libertad informativa o autodeterminación informativa.[158]

En cuanto al objeto protegido por este nuevo derecho, este sería «garantizar la facultad de las personas para: conocer y acceder a las informaciones que les conciernen archivados en bancos de datos (lo que se denomina *habeas data* por su función análoga en el ámbito de la información a cuanto supuso el tradicional *habeas corpus* en lo

[156] Cfr. SERRANO PÉREZ, *El derecho fundamental…,* op. cit., p. 76.
[157] Ídem. Esta dualidad también la recoge RUIZ MIGUEL, para quién el derecho a la intimidad informática recoge, por una parte, una serie de deberes positivos para los poderes públicos u organismos que proceden al tratamiento automatizado de datos personales, —sería lo que se entiende por los principios de la calidad de datos—, y por otra, una serie de mecanismos de tutela para los ciudadanos.
[158] En el mismo sentido véase, Mª Mercedes SERRANO PÉREZ, *El derecho fundamental a la protección de datos…,* op. cit. p. 76.

referente a la libertad personal); controlar su calidad, lo que implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados; y disponer sobre su transmisión».[159]

La libertad informática se configura como un derecho fundamental, que tiene por objeto garantizar a las personas individuales y en su caso colectivas, el derecho a: a) la información, esto es, la posibilidad de conocer los bancos de datos existentes, así como su titularidad y finalidad; b) el control, que se desglosa, a su vez, en la facultad de acceso por parte de los afectados a las informaciones que les conciernen. Además, el control comprende la facultad de corrección y cancelación de los datos inexactos o procesados indebidamente; y por último, c) la tutela de las facultades anteriores mediante el establecimiento de los oportunos recursos.[160]

El *habeas data*, en cuanto facultad para conocer y acceder a la información personal que nos concierna, que se encuentren en los bancos de datos públicos o privados, se configura como «el cauce procesal para salvaguardar la libertad de la persona en la esfera informática».[161] Esta figura surge como un símil del *habeas corpus*. En efecto, el *habeas corpus*, surgió como una garantía de defensa frente a la libertad física, frecuentemente sometida a privaciones abusivas. En la sociedad actual la libertad de la persona también se ve amenazada, no tanto en su vertiente física, sino en su aspecto más inmaterial, espiritual o intangible, mediante las informaciones personales sobre un individuo que puede convertirse en una amenaza para su manera de actuar, en definitiva, para su libertad.[162]

Respecto de la relación entre el derecho a autodeterminación informativa o libertad informática y el derecho a la intimidad, los autores no rechazan de forma total la relación entre ambas, pues la conexión es evidente. Es más, se ha afirmado que «el

[159] Cfr. A. E. PÉREZ LUÑO, «El derecho a la autodeterminación…», op. cit., p. 304, que remite a su obra *Nuevas tecnologías, sociedad y derecho. El impacto socio-jurídico de las N. T. de la información*, Fundesco, Madrid, 1987, p. 87

[160] Ídem.

[161] Ibídem, p. 45.

[162] Al respecto SERRANO PÉREZ, observa que «el *habeas data* no se concibe como un procedimiento de protección de la intimidad sino como una garantía para asegurar algo más, nada menos que la libertad». Cfr. *El derecho fundamental…*, op. cit., p. 75.

derecho a la autodeterminación informativa se construye a partir del derecho a la intimidad».[163]

No obstante, estamos de acuerdo con aquellos que plantean que el ordenamiento constitucional español «acoge una idea del derecho a la intimidad que no se extiende a lo que se ha denominado protección de datos».[164] Recordemos que la técnica de protección de datos es más amplia que el concepto de intimidad, ya que faculta para excluir u oponerse a la recolección no autorizada de datos, aun cuando estos no afecten ese ámbito o círculo personalísimo que protege la intimidad.[165] Ello es así, porque aun cuando se conciba el derecho a la intimidad como un derecho amplio, elástico, dinámico que permita ampliar su cobertura para dar cabida a la protección de las personas ante nuevos riesgos y amenazas, no ha podido constituirse en un medio idóneo para la tutela jurídica de la personas frente a los problemas que presenta la informática, ni las TIC en general.[166]

El proceso de construcción doctrinal del derecho a la protección de datos (autodeterminación informativa) como un derecho autónomo y con perfiles propios, que lo diferencia de otros derechos destinados al resguardo de la personalidad, planteó la necesidad de una interpretación teleológica y no meramente literal del artículo 18.4 CE. Así, buscando el sustrato de fondo se desea proteger, fue necesario recurrir a un contenido distinto del plasmado en el texto constitucional, con el fin de reconducir a él satisfactoriamente todos los inconvenientes derivados del uso de los ordenadores. Para ello se postuló que el reconocimiento constitucional a la necesidad de limitar el uso de la informática constituye un auténtico derecho fundamental, que comprende un conjunto de facultades y posibilidades del individuo que no pueden ser absorbidas en las categorías que expresamente se recogen en otros apartados (1, 2 y 3) del artículo 18 CE. De todo ello, se concluye que «la intimidad y el honor no son idóneos para suministrar el soporte material sobre el que descansa la técnica de la protección de datos».[167]

---

[163] Al respecto, véase Pablo LUCAS MURILLO DE LA CUEVA, *El derecho a la autodeterminación informativa*, op. cit. p. 45. Este mismo autor, realiza en la citada obra un proceso de reconstrucción del derecho a la intimidad como base para analizar la autodeterminación informativa. Véase pp.45-99.
[164] Ibídem., p. 97.
[165] Ibídem., pp. 97 y 98.
[166] Ibídem., pp. 98 y 99.
[167] Cfr. Pablo LUCAS MURILLO DE LA CUEVA, «La protección de los datos personales ante el uso de la informática en el derecho español (II)», *Estudios de Jurisprudencia*, año 1, núm. 3, enero-febrero 1992, p. 14. En el mismo sentido véase SERRANO PÉREZ, *El derecho fundamental…*,op. cit., p. 77.

Vistos los principales lineamientos doctrinarios en el proceso de construcción del derecho fundamental a la protección de datos como derecho autónomo, pasaremos a constatar que existe una estrecha relación entre la evolución de la dogmática con la evolución legislativa en España.

Las primeras reflexiones teóricas, se producen de forma prácticamente simultánea a la elaboración de la Constitución.[168] En el intervalo que media entre la entrada en vigencia de la Constitución Española y la primera regulación de la protección de datos personales en 1992, no existió un auténtico debate sobre la cuestión.[169] Lo anterior cambia con la aprobación de la Ley Orgánica 5/1992, de 29 de octubre de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD)[170], la cual, se sirvió del Convenio 108 y de las Pautas de la Directiva europea sobre la materia, entonces en gestación.[171]

[168] Al respecto, véase Antonio Enrique PÉREZ LUÑO, «La protección de la intimidad frente a la informática en la Constitución española de 1978», *Revista de Estudios Políticos (Nueva Época)*, núm 9, mayo-junio, 1979, pp. 73 y ss; «La juscibernética en España», en R. J. C, 1972, núm. 2, pp. 303 y sigs.; *Cibernética, informática y derecho. Un análisis metodológico,* Publicaciones del Real Colegio de España, Bolonia, 1976, pp. 133 y ss.

[169] Al respecto Pablo LUCAS MURILLO DE LA CUEVA, señala que « Lo anterior, llama la atención toda vez que en el ámbito supranacional europeo, el Consejo de Europa ya se había aprobado el Convenio núm. 108, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, que establecía los principios esenciales sobre los que descansa este derecho». Agrega que una explicación plausible, podría ser «la actitud tomada por los Tribunales españoles, los que no obstante, la fórmula abierta y transversal con que se redactó el artículo 18.4 de la constitución Española, que facilitaba la recepción y desarrollo del citado Convenio le negaron valor al mismo para sustentar derechos, al considerar que éste se limitaba a consagrar principios que debían concretar los legisladores nacionales, sus únicos destinatarios». Cfr. «La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad», op. cit., p. 20.

[170] Publicada en el BOE núm. 262 de 31.10.1992. Una de las notas que destacan los autores al referirse a la LORTAD, fue que encuadró el tema que regulaba bajo la idea de *privacidad*, como expresamente señalaba su exposición de motivos, que señalaba: «en este caso, al desarrollar legislativamente el mandato constitucional de limitar el uso de la informática, se está estableciendo un nuevo y más consistente ***derecho a la privacidad de las personas***» [el destacado es nuestro]. El problema era que el artículo 1 de la LORTAD, al hablar del objeto de la ley, reiteraba el apartado cuarto del artículo 18 de la Constitución española, con lo que mantenía «cierta ambigüedad entorno a la trascendencia del paso que estaba dando». Cfr. Pablo LUCAS MURILLO, «La construcción del derecho a la autodeterminación… », op. cit., pp. 21-23.

[171] LUCAS MURILLO, dice que «si bien los fundamentos de su regulación —y del derecho al que da cuerpo— se elevan, en última instancia, a la dignidad humana y se vinculaban a la personalidad individual, fueron motivos más prosaicos los que impulsaron la aprobación de este texto legal: la puesta en marcha de los Acuerdos de Schengen». Cfr. «La construcción del derecho a la autodeterminación… », op. cit., pp. 21 y 22.

Con la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)[172], se resolvió el problema prescindiendo de exposición de motivos y estableciendo en su artículo 1 que su objeto es: «… 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». Es importante el cambio de planteamiento que refleja este último precepto, porque no se sitúa en el marco de la limitación del uso de la informática, ni siquiera en el del artículo 18.4 de la Constitución, como sí hacía la LORTAD, sino como una garantía para todas las libertades y derechos fundamentales.[173] Lo anterior, se ratificaría un año después con el contenido de las Sentencias 290/2000 y 292/2000 del Tribunal Constitucional español, que pasamos a revisar a continuación.

3.2. Jurisprudencia del Tribunal Constitucional de España

La configuración del derecho fundamental a la protección de datos personales como un derecho autónomo e independiente de otros institutos jurídicos afines, es el fruto de un largo proceso evolutivo, donde la doctrina, la legislación (nacional y europea) y jurisprudencia han jugado un papel central. Pero será esta última, la que luego de más de veinte años desde la entrada en vigor de la Constitución Española en diciembre de 1978, consolide definitivamente este derecho mediante dos Sentencias del Tribunal Constitucional (STC 290/2000[174] y STC 292/2000[175]), ambas de 30 de noviembre de 2000.[176]

---

[172] Publicada en el BOE núm. 298 de 14.12.1999

[173] LUCAS MURILLO, desliza una crítica respecto de la actitud tomada por el legislador, al señalar que «si se pensaba que con el texto de 1999 se superaba el marco de la limitación del uso de la informática para una normativa que va más allá de tal objetivo, además de que se podía haber dicho sin ninguna dificultad, sucede que ese propósito es igualmente perseguible desde el mismo precepto constitucional que se preocupa de la garantía del pleno ejercicio de los derechos de los ciudadanos, de todos sus derechos». Al fin y al cabo, continúa , «no cuenta trabajo ver en ese último apartado del artículo 18 la voluntad de protegerlos de los peligros derivados de las tecnologías de la información, ya estrechamente vinculadas, por otra parte, a las de las comunicaciones». Cfr. «La construcción del derecho a la autodeterminación… », op. cit., pp. 24.

[174] La Sentencia 290/2000, de 30 de noviembre, publicada en el BOE núm.4 (Suplemento) de 4.01.2001, soluciona la discusión suscitada por el Gobierno y el Parlamento de Cataluña con el Estado. El Tribunal resolvió que el bien jurídico protegido por el artículo 18.4 no es el reparto competencial sino el derecho fundamental a la protección de datos personales que debe imponerse incluso sobre aquel. Además, señala que el ámbito competencial general en todo el Estado, que corresponde a la Agencia Española de Protección de Datos, se exige por la necesidad de garantizar la protección en términos de igualdad

Antes de pasar al análisis de dichos fallos, revisaremos brevemente, las principales Sentencias del TCE, sobre protección de datos, a objeto de ver la evolución de los criterios adoptados por dicho Tribunal. Lo primero que podemos constatar es que las Sentencias anteriores a las del 30 de noviembre de 2000 no siguieron la misma línea en lo que se refiere a la identificación del derecho, cuyo amparo estaba dispensando.[177]

La primera Sentencia del TCE sobre protección de datos personales, es la STC 254/1993, de 20 julio.[178] En ella se estableció el derecho de los ciudadanos a conocer los datos personales que le conciernen y que se hallan registrados en archivos administrativos informatizados. Entre sus argumentos se destaca por un lado, que acoge la dimensión positiva del derecho a la intimidad como facultad de control sobre los datos relativos a la propia persona, y acepta las nociones de libertad informática y *habeas data* como integrantes de la garantía de la intimidad frente a la informática, consagrada en el art. 18.4 de la CE. Por otra parte, el fallo reconoce la aplicación inmediata de los derechos fundamentales, sin que sea necesario un desarrollo legislativo para su plena eficacia, en este caso, de la libertad informática, que recoge el artículo 18.4 CE.[179]

---

territorial. Con ello, el Tribunal confirmó la constitucionalidad de la opción realizada por la LORTAD (1992) y mantenida por la LOPD (1999) de atribuir competencia exclusiva sobre los ficheros de titularidad privada a la Agencia Española de Protección de Datos.

[175] La Sentencia 292/2000, de 30 de noviembre, se pronunció sobre el Recurso de inconstitucionalidad presentado por el Defensor del Pueblo, respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Publicada en el BOE núm. 4 (Suplemento) de 4.1. 2001.

[176] Sobre la jurisprudencia del Tribunal Constitucional Español en materia de protección de datos personales, existe una abundante bibliografía, véase entre otros: Antonio TRONCOSO REIGADA, «La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional», en *Cuadernos de Derecho Público*, nº 19-20, monográfico sobre *Protección de Datos*, 2003, pp. 231-334; Ernesto QUILEZA AGRADA, «El derecho a la protección de los datos en la jurisprudencia constitucional», en III Jornadas sobre informática y sociedad, coord. por Miguel Angel Davara Rodríguez, Madrid, 2001, pp. 187-196; Ana Isabel HERRÁN ORTIZ, «La protección de datos personales en la jurisprudencia constitucional», en *Estudios jurídicos en memoria de José María Lidón*, coord. por Juan Ignacio Echano Basaldúa, Universidad de Deusto, 2002, pp. 985-1000; Ignacio VILLAVERDE MENÉNDEZ, «La jurisprudencia del Tribunal Constitucional sobre el derecho fundamental a la protección de datos de carácter personal», en *La protección de datos de carácter personal en los centros de trabajo*, coord. por Antoni Farriols i Solá, 2006, pp. 48-63.

[177] Cfr. Pablo LUCAS MURILLO DE LA CUEVA, «La construcción del derecho a la autodeterminación…», op. cit., pp. 31 y 32.

[178] En este caso el recurrente, solicitaba que se comunicara la existencia, finalidad y responsables de los ficheros automatizados dependientes de la Administración del Estado donde obrasen datos personales suyos. Publicada en el BOE núm. 197, de 18 de agosto de 1993.

[179] Al respecto, véase Concepción CONDE ORTÍZ, *La protección de datos personales*, Dykinson, Madrid, 2005, pp. 40 y 41; y Antonio ORTI VALLEJO, «El nuevo derecho fundamental (y de la

Realizando una interpretación bastante literal del precepto constitucional, el fallo señala 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 informática» (STC 254/1993, fundamento jurídico 6º).

Si bien el Tribunal reconoce que tras el artículo 18.4 de la CE subyace algo que no es exactamente igual al derecho a la intimidad, mantiene la misma línea de relativa ambigüedad que caracteriza la exposición de motivos de la LORTAD y su opción por el término *privacidad* en un intento de eludir la toma de postura en el debate sobre el bien jurídico subyacente.[180] En definitiva, en esta sentencia aún no se configura el derecho a la protección de datos como un derecho autónomo respecto de la intimidad.

En la Sentencia posterior STC 143/1994[181] deshará esa indefinición y razonará desde el punto de vista del derecho a la intimidad. Luego, en las SSTC de 1998[182] y en las SSTC de 1999[183], preparará el camino que conduce a la STC 202/1999, de 30 de noviembre. En ellas el Tribunal señala sobre el derecho previsto en el artículo 18.4 CE, que:

> «El artículo 18.4 CE no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, como ha quedado dicho, sino que además consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona —a la privacidad según la expresión utilizada por la derogada LORTAD— pertenezcan o no al ámbito más estricto de la intimidad para así preservar el pleno ejercicio de sus derechos. La sentencia consagra un derecho fundamental autónomo cuya finalidad es el control de informaciones que conciernen a cada persona» (STC 11/1998, fundamento jurídico 6º).

---

personalidad) a la libertad informática (a propósito de la STC 254/1994, de 20 de julio)», *Derecho privado y Constitución*, núm. 2, enero-abril, 1994, p. 305.

[180] Pablo LUCAS MURILLO DE LA CUEVA, «La construcción del derecho a la autodeterminación…», op. cit., p. 32.

[181] Publicada en el BOE núm. 140 de 13.6.1994

[182] SSTC 11, 33, 35, 45, 60, 77, 94, 104, 105, 106, 123, 124, 125, 126, 158, 198, 223 de 1998.

[183] SSTC 30, 44, 45 y 202 de 1999.

«Se trata, por tanto, de 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 automatizado de datos» (SSTC 254/1993, fundamento jurídico 6º y 11/1998, fundamento jurídico 4º).

Añade el TCE:

«la garantía de la intimidad adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona; la llamada "libertad informática" es así 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 aquel legítimo que justificó su obtención» (STC 254/1993, fundamento jurídico 7º; STC 11/1998, fundamento jurídico 4º; STC 94/1998, fundamento jurídico 4º).

Como hemos señalado anteriormente, será con la STC 292/2000, de 30 de noviembre, donde el TCE despejará las ambigüedades y establecerá rotundamente que el derecho a la protección de datos es un derecho autónomo e independiente. De esta forma, pasa de ser considerado un «instituto de garantía de los derechos a la intimidad y el honor y del pleno disfrute de los restantes derechos de los ciudadanos», a constituirse, también, en «un derecho fundamental».[184] En este fallo, el Tribunal no solo reconoce la existencia del derecho a la protección de datos como Derecho autónomo e independiente del Derecho a la intimidad, sino que también determina su contenido esencial, lo relaciona con el artículo 18.4 y 10.2 de la Constitución y, además, cita de forma expresa diversos instrumentos internacionales que regulan la materia como soporte del fallo.[185]

La sentencia diferencia claramente el derecho a la intimidad del artículo 18.1 y el derecho a la protección de datos del artículo 18.4 de la CE. El Tribunal señala que, si bien ambos comparten «el objetivo de ofrecer una eficaz protección constitucional de la

[184] Cfr. Pablo LUCAS MURILLO DE LA CUEVA, «La construcción del derecho a la autodeterminación…», op. cit., pp. 33 y 34.
[185] José Luis PIÑAR MAÑAS, "Protección de datos: origen, situación actual y retos de futuro", en *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, pp. 97 y 98.

vida privada personal y familiar», se distinguen porque la protección de datos «atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley». Pero no cualquier Ley, sino aquella que «conforme al artículo 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE)».[186] Añade el fallo, que la peculiaridad de este derecho fundamental respecto del derecho a la intimidad radica en la distinta función que cumple, diferencia que se proyecta sobre su objeto y contenidos respectivos.[187]

Así, la función del derecho a la intimidad es la de protegernos frente a cualquier invasión del ámbito de la vida personal y familiar que deseamos excluir del conocimiento ajeno y de las intromisiones de terceros en contra de nuestra voluntad, mientras que el derecho a la protección de datos persigue garantizarnos un poder de control sobre nuestros datos personales, sobre su uso y destino, a fin de impedir su tráfico ilícito y lesivo para nuestra dignidad y derechos.[188] En otros términos, la función del derecho a la intimidad permite excluir ciertos datos de la persona del conocimiento ajeno, mientras el derecho a la protección de datos garantiza a los individuos un poder de disposición sobre sus datos. Este poder de disposición, nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes lo poseen y con qué fin.[189]

---

[186] Cfr. Pablo LUCAS MURILLO DE LA CUEVA, «La construcción del derecho a la autodeterminación…», op. cit., p. 34.

[187] LUCAS MURILLO DE LA CUEVA, observa que «La sentencia, señala que *la singularidad del derecho a la protección de datos* viene, de una parte, de la mayor amplitud de su objeto en comparación con el del derecho a la intimidad, ya que "extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el artículo 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 (…), como el derecho al honor, (…) e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona". De esta manera, el derecho fundamental a la protección de datos "amplía la garantía constitucional a aquellos de esos datos que sean relevantes o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar o cualquier otro bien constitucionalmente amparado"». Cfr. «La construcción del derecho a la autodeterminación…», op. cit., pp. 35 y 36.

[188] Cfr. Pablo LUCAS MURILLO DE LA CUEVA, «La construcción del derecho a la autodeterminación…», op. cit., pp. 34 y 35.

[189] En la misma línea argumentativa, véase Concepción CONDE ORTÍZ, *La protección de datos personales*, Dykinson, Madrid, 2005, pp. 45 y 46.

Otra diferencia entre intimidad y protección de datos es su objeto. El derecho a la protección de datos, tiene un objeto más amplio que el derecho a la intimidad, ya que no se reduce a los datos íntimos de la persona, sino a cualquier dato personal, sea íntimo o no, ya que su objeto no es sólo la intimidad individual, sino los datos de carácter personal.[190] Al respecto el fallo señala:

> «…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. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo» (STC 292/2000, fundamento jurídico 6º).

En cuanto al contenido del derecho a la protección de datos, este consiste en un poder de disposición y control de los datos personales, que se concreta en la facultad de consentir sobre la recogida y el uso de sus datos personales y a saber de los mismos: saber, por tanto, qué datos se poseen sobre su persona y qué destino han tenido. Comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención.[191]Además, comprende el derecho a ser informados, a consentir, así como los derechos de acceso, rectificación y cancelación, todos los cuales integran el derecho fundamental a controlar la recogida y el uso de aquellos datos personales que puedan poseer tanto el Estado y otros entes públicos como los particulares.[192]

Respecto de los límites al derecho a la protección de datos, el fallo dispone:

---

[190] Ídem.
[191] STC 11/1998, fundamento jurídicos 5º y STC 94/1998, fundamento jurídico 4º.
[192] STC 292/2000, fundamentos jurídicos 2, 5 y 7.

> «En cuanto a los límites de este derecho fundamental no estará de más recordar que la Constitución menciona en el art. 105 b) que la ley regulará el acceso a los archivos y registros administrativos "salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas" (en relación con el art. 8.1 y 18.1 y 4 CE), y en numerosas ocasiones este Tribunal ha dicho que la persecución y castigo del delito constituye, asimismo, un bien digno de protección constitucional, a través del cual se defienden otros como la paz social y la seguridad ciudadana. Bienes igualmente reconocidos en los arts. 10.1 y 104.1 CE (por citar las más recientes, SSTC 166/1999, de 27 de septiembre, FJ 2, y 127/2000, de 16 de mayo, FJ 3.a; ATC 155/1999, de 14 de junio). Y las SSTC 110/1984 y 143/1994 consideraron que la distribución equitativa del sostenimiento del gasto público y las actividades de control en materia tributaria (art. 31 CE) como bienes y finalidades constitucionales legítimas capaces de restringir los derechos del art. 18.1 y 4 CE» (STC 292/2000, considerando 9º).

El Convenio Europeo de 1981 también ha tenido en cuenta estas exigencias en su art. 9. Al igual que el Tribunal Europeo de Derechos Humanos, quien refiriéndose a la garantía de la intimidad individual y familiar del art. 8 CEDH, aplicable también al tráfico de datos de carácter personal, reconociendo que pudiera tener límites como la seguridad del Estado[193], o la persecución de infracciones penales[194], ha exigido que tales limitaciones estén previstas legalmente y sean las indispensables en una sociedad democrática. Lo anterior implica que la ley que establece esos límites sea accesible al individuo concernido por ella, que resulten previsibles las consecuencias que para él pueda tener su aplicación, y que los límites respondan a una necesidad social imperiosa y sean adecuados y proporcionados para el logro de su propósito.[195]

Por tanto, si bien la Constitución no le impone límites específicos, ni remite a los poderes públicos para su determinación, los límites al ejercicio del derecho a la protección de datos han de encontrarse en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos.[196] Estos límites, deben ser los indispensables para la convivencia en una sociedad democrática, venir regulados por la ley y cumplir con los requisitos de proporcionalidad y finalidad. Sobre este último punto, el fallo hace una remisión, tanto a la propia Constitución, como a instrumentos internacionales

[193] STEDH caso *Leander*, de 26 de marzo de 1987, §§ 47 y ss.
[194] *Mutatis mutandis*, SSTEDH, casos *Z*, de 25 de febrero de 1997, y *Funke*, de 25 de febrero de 1993.
[195] SSTEDH, caso *X* e *Y*, de 26 de marzo de 1985; caso *Leander*, de 26 de marzo de 1987; caso *Gaskin*, de 7 de julio de 1989; mutatis mutandis, caso *Funke*, de 25 de febrero de 1993; caso *Z*, de 25 de febrero de 1997.
[196] En el mismo sentido, véase Pablo LUCAS MURILLO DE LA CUEVA, «La construcción del derecho a la autodeterminación…», op. cit., p. 47.

(Convenio núm. 108) y a la jurisprudencia del Tribunal Europeo de Derechos Humanos, para graficar que existen ciertos bienes y finalidades constitucionales que permiten la restricción de este derecho, siempre cuando dichas limitaciones sean indispensables en una sociedad democrática.

La STC 292/00, con el objeto de confirmar el significado y contenido del derecho a la protección de datos hace referencia a los instrumentos internacionales que se refieren a este derecho fundamental. Menciona la Resolución 45/95 de la Asamblea General de Naciones Unidas que recoge la versión revisada de los Principios Rectores aplicables a los Ficheros Computarizados de Datos Personales; el Convenio núm. 108 para la Protección de las Personas respecto al Tratamiento Automatizado de Datos de Carácter Personal, hecho en Estrasburgo el 28 de enero 1981; la Directiva 95/46, sobre Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y la Libre Circulación de estos datos; y la Carta de Derechos Fundamentales de la Unión Europea. Como señala Lucas Murillo, «la sentencia subraya que todos estos textos coinciden en el establecimiento de un régimen jurídico para la protección de datos personales basado en la predisposición de un haz de garantías para los afectados, semejante al que ha descrito [la propia sentencia], que hace posible su respeto».[197]

En resumen, en la Sentencia 292/2000, el Tribunal Constitucional español, realiza un completo análisis de este derecho fundamental, indicando su objeto, contenido y límites. Además, indica su singularidad sobre otros derechos que reconoce el artículo 18.1 CE y lo diferencia expresamente del derecho a la intimidad. Por último, reconoce la virtualidad interpretativa que para precisar dicho derecho ofrecen los textos internacionales y comunitarios.

Desde estas premisas, la Sentencia del TCE 292/2000 resuelve el recurso de inconstitucionalidad presentado por el Defensor del Pueblo y declara inconstitucionales las comunicaciones de datos entre ficheros de las Administraciones Públicas cuando carezcan de consentimiento del afectado o de previsión legal (artículo 21 LOPD). También, declara inconstitucional las limitaciones del artículo 24.2 al ejercicio de los derechos de acceso, rectificación y cancelación en los ficheros de titularidad pública, así

[197] Cfr. Pablo LUCAS MURILLO DE LA CUEVA, «La construcción del derecho a la autodeterminación…», op. cit., p. 39.

como la previsión del primer apartado de ese mismo artículo que excluía el deber de informar al afectado en la recogida de datos para esos mismos ficheros cuando impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas y cuando afecte a la persecución de infracciones administrativas.

La otra Sentencia dictada en la misma fecha por el TCE (STC 290/2000), confirmó la constitucionalidad de la opción realizada por la LORTAD y mantenida por la LOPD de atribuir la competencia exclusiva sobre los ficheros de titularidad privada a la Agencia Española de Protección de Datos.

Si analizamos retrospectivamente los fallos del Tribunal Constitucional español en materia de protección de datos, no puede negarse que el cambio de criterio y la evolución que tuvo respecto de este derecho, vino de la mano, tanto de las aportaciones doctrinales anteriores que venían propugnando la autonomía de este derecho, como del desarrollo legislativo que brindó la LORTAD y luego la LOPD al artículo 18.4. Así también, no puede desconocerse el soporte que le brindaron los instrumentos internacionales sobre la materia y la jurisprudencia del Tribunal Europeo de Derechos Humanos.[198]

Como siempre ocurre en el nacimiento y/o evolución de cualquier derecho fundamental, es la confluencia de factores de distinta naturaleza (social, política y cultural) los que fuerzan una respuesta jurídica (doctrinal, jurisprudencial, legal) a los nuevos problemas que aquejan a la sociedad. En este caso, todos estos factores llevaron a reconocer un nuevo derecho fundamental: el derecho a la protección de datos de carácter personal, como categoría autónoma y distinta del derecho a la intimidad en el ordenamiento jurídico español.

[198] Al respecto, LUCAS MURILLO DE LA CUEVA, señala que «es llamativo que la primera Sentencia sobre el derecho a la protección de datos —la STC 254/1993— no se dicte sino pocos meses después de la entrada en vigor de la LORTAD y que la 11/1998 y las que componen la serie que ésta encabeza surjan cuando se discute la transposición de la Directiva 46/95/CEE». En fin, continúa LM, «las de 30 de noviembre de 2000, no sólo cuentan ya con el referente de destacadas decisiones del Tribunal de Estrasburgo, sino que aparecen casi a la par que la Carta de los Derechos Fundamentales de la Unión Europea». Cfr. «La construcción del derecho a la autodeterminación…», op. cit., p. 43.

Por último, si evaluamos la doctrina, legislación y jurisprudencia de los tres países que han sido objeto de este estudio, podemos concluir que en todos ellos se ha alcanzado un gran nivel de protección de los datos de carácter personal frente al uso de la informática. En este proceso han influido diferentes factores, entre los que destaca: el debate promovido desde ámbitos académicos y sociales sobre el bien jurídico protegido con este derecho y, en particular, sobre la diferencia existente entre intimidad y autodeterminación informativa; la progresiva elaboración desde el espacio europeo, a partir del Convenio n.º 108 del Consejo de Europa, de una disciplina orientada a proteger los datos personales, que acabará plasmada en la Directiva 95/46/CE, donde se fijan los principios, derechos y obligaciones esenciales mínimos que rigen la materia; el paso dado por la Unión Europea en el 2000 con la Carta de los Derechos Fundamentales, al reconocer la autonomía del derecho a la protección de datos de carácter personal. Además, si reparamos en el texto del Tratado de Lisboa (que reemplazó a la fallida Constitución para Europa), veremos que no sólo lo reconoce como fundamental, sino que da un paso adicional e incluye su respeto entre los elementos de la vida democrática de la Unión; la jurisprudencia, tanto de los Tribunal Constitucionales y Superiores de los respectivos países, como la del Tribunal Europeo de Derechos Humanos que, a partir del derecho a la vida privada reconocido por el artículo 8 de la Convención, dotó de autonomía a la protección de datos de carácter personal. Por tanto, el escenario que tenemos a la vista en Europa en general y en estos tres países estudiados en particular, puede verse «como el punto de llegada o la meta a la que apuntaban las iniciativas que, desde mediados de los años ochenta, reclamaban la protección frente al avance tecnológico, y muy particularmente frente al uso de la informática».[199]

[199] Cfr. Pablo LUCAS MURILLO DE LA CUEVA, «Perspectivas del derecho a la autodeterminación informativa». En: «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 5. UOC, 2007, p. 20. <http://www.uoc.edu/idp/5/dt/esp/lucas.pdf> [Fecha de consulta: 16.7.2011].

CAPÍTULO TERCERO
DIRECTRICES INTERNACIONALES SOBRE PROTECCIÓN DE DATOS PERSONALES

SUMARIO: INTRODUCCIÓN; 1. LAS RECOMENDACIONES DE LA ORGANIZACIÓN PARA LA COOPERACIÓN Y DESARROLLO ECONÓMICO (OCDE); 1.1. Directrices de la OCDE sobre protección de la privacidad y el flujo transfronterizo de datos personales (1980); 1.1.1. *Origen, importancia y fundamento*; 1.1.2. *Estructura y contenido*; 1.2. Otras Recomendaciones de la OCDE en materia de privacidad; 2. DIRECTRICES DE LA ONU PARA LA REGULACIÓN DE LOS ARCHIVOS DE DATOS PERSONALES INFORMATIZADOS; 3. FORO DE COOPERACIÓN ECONÓMICA ASIA-PACÍFICO (APEC); 3.1. Marco de Privacidad (2004); 3.2. Reglas de privacidad transfronteriza (2007); 4. LA NECESIDAD DE UN INSTRUMENTO JURÍDICO UNIVERSAL Y VINCULANTE; 4.1. Justificación de la necesidad de un nuevo instrumento; 4.2. Los Estándares internacionales sobre privacidad y protección de datos. Un primer paso hacia un Convenio Universal.

INTRODUCCIÓN

El respeto por la privacidad y la protección de datos personales, dista mucho de ser uniforme en el mundo. Por el contrario, existen profundas diferencias en cuanto al nivel de protección brindado a este derecho por los distintos Estados, que obedecen a distintos motivos, como son, entre otros, las diferencias en cuanto al nivel de desarrollo económico, social y cultural, como también las discrepancias entre distintos sistemas jurídicos. Así tenemos que al día de hoy, avanzado ya el siglo XXI, existen Estados donde no existe ningún tipo de garantía a este respecto y otros, por el contrario, donde se dan los más altos niveles de protección.[200]

[200] Cabe tener presente que también existe una situación intermedia, es decir países que poseen una legislación general o especial sobre la materia, pero con tales falencias que difícilmente podrían ser catalogadas como una garantía suficiente para resguardar los derechos de las personales en lo que respecta al tratamiento de sus datos personales. Un ejemplo de esta última situación la representa el Estado chileno, que dictó la primer ley sobre protección de datos personales en Latinoamérica, la Ley N° 19.628, de 18 de agosto de 1999. No obstante, si se analiza su contenido, encontramos múltiples

Es necesario entonces encontrar una base mínima, que sirva de orientación a los Estados sobre esta materia. En este sentido, el desarrollo de reglas internacionales que garanticen, de un modo uniforme, el respeto a la protección de datos y a la privacidad resulta prioritario.[201] La adopción de Recomendaciones y Directrices elaboradas por organizaciones internacionales como la ONU, APEC, OCDE y regionales como la Red Iberoamericana de Protección de Datos, contribuyen a la creación de marcos internacionales que permitan impulsar el respeto a la privacidad y la protección de datos, lo cual supone un positivo avance de cara a lograr un estándar mínimo de principios, derechos y obligaciones de carácter universal que rijan la materia.

Hasta el momento seis son los principales instrumentos internacionales que existen sobre la materia: 1) las Directrices del Consejo de la Organización para la Cooperación y el Desarrollo Económico (en adelante, la OCDE), sobre protección de la privacidad y el flujo transfronterizo de datos personales, de 23 de septiembre de 1980; 2) el Convenio número 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981; 3) las Directrices de Naciones Unidas, para la regulación de los archivos de datos personales informatizados, de 14 de diciembre de 1990; 4) la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, de 24 de octubre de 1995; 5) el Marco de Privacidad (*Privacy Framework*) del Foro de Cooperación Económica Asia Pacífico (en adelante, APEC), de noviembre de 2004; y 6) la Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el tratamiento de datos de carácter personal, acogida favorablemente por la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (Resolución de Madrid), de 5 de noviembre de 2009.

---

falencias, entre las que destacan el hecho de no regular la transferencia internacional de datos personales y no establecer una autoridad de control autónoma encargada de vigilar el debido cumplimiento de la ley. Para un análisis crítico de la Ley 19.628, véase Pedro ANGUITA RAMÍREZ, *La protección de datos personales y el derecho a la vida privada". Régimen jurídico, jurisprudencia y derecho comparado.* Santiago de Chile: Editorial Jurídica de Chile, 2007; Raúl ARRIETA CORTÉS (Coord.), *Reflexiones Sobre el Uso y Abuso de los Datos Personales en Chile*, Expansiva, Santiago de Chile, 2011; Claudio MAGLIONA MARKOVICTH, «Breve análisis de la Ley N° 19.628, sobre Protección de la Vida Privada», Revista Electrónica de Derecho Informático, N°29, diciembre de 2000.

[201] Frédéric BLAS, «Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales», Revista Derecho del Estado n.º 23, diciembre de 2009, pp. 63 y 64.

Los instrumentos jurídicos señalados, se pueden clasificar, por una parte, atendiendo a su grado de **obligatoriedad** y, por otra, a su **objeto** principal.

Respecto del primer criterio, las Directrices de la OCDE, de las Naciones Unidas, el Marco de Privacidad de la APEC y los estándares internacionales de la Resolución de Madrid, carecen de fuerza jurídica vinculante, constituyen simplemente instrumentos orientativos de la actividad de los Estados Miembros en materia de protección de datos y privacidad, sin perjuicio de las recomendaciones que los mismos contienen de cumplir los principios establecidos en esos textos. En cambio, tanto la Directiva 95/46/CE, como el Convenio nº 108 del Consejo de Europa, resultan de obligado cumplimiento para los Estados Miembros de la Unión Europea y para quienes ratifiquen el Convenio respectivamente.[202]

El otro criterio de distinción entre este tipo de instrumento, dice relación con la finalidad principal que persiguen. El Convenio nº 108, las Directivas de la Naciones Unidas y los Estándares internacionales de 2009, tienen por objeto principal regular y garantizar el derecho fundamental de los ciudadanos a la protección de sus datos personales. Por su parte, las Directrices de la OCDE, de la APEC y de la Directiva 95/46/CE tienen por fin el establecimiento de una regulación básica de protección de datos que garantice el libre flujo de la información entre los Estados participantes en las mismas.[203]

Ahora pasaremos a revisar sucintamente, el contenido de cada uno de estos instrumentos jurídicos en el ámbito internacional, a objeto de tener claridad respecto de sus fundamentos, objetivos y elementos esenciales relativos a la protección de datos personales.

[202] Una distinción similar la encontramos en Agustín, PUENTE ESCOBAR, «Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal», en *Protección de Datos de Carácter Personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos, La Antigua – Guatemala, 2-6 de junio de 2003)*, Tirant lo Blanch, Valencia, 2006, pp. 50 y 51.

[203] En el mismo sentido, pero utilizando la expresión «fundamento jurídico», para referirse a la mismo, véase Agustín, PUENTE ESCOBAR, op. cit., p. 51.

1. LAS RECOMENDACIONES DE LA ORGANIZACIÓN PARA LA COOPERACIÓN Y DESARROLLO ECONÓMICO (OCDE)

La OCDE, tuvo su origen en el Convenio firmado en París el 14 de diciembre de 1960[204]. Tiene por objeto promover políticas de expansión de las economías de los Estados miembros, elevar su nivel de empleo y mejorar la calidad de vida de sus ciudadanos, manteniendo la estabilidad financiera. Asimismo, busca contribuir al desarrollo de la economía y a la expansión del comercio mundial. Actualmente la componen más de treinta Estados desarrollados y en vías de desarrollo, los que en su conjunto representan el 70% del mercado mundial y el 80% del Producto Nacional Bruto (PNB) mundial.[205] Los países miembros comparten tres principios básicos: democracia pluralista, respeto de los derechos humanos y economías de mercado abiertas.[206]

Este foro ha servido a los gobiernos para analizar y establecer orientaciones sobre temas de relevancia internacional, compartiendo experiencias y buscando soluciones a problemas comunes. La preocupación de la OCDE sobre el tema de la protección de la privacidad y los datos personales se debe, esencialmente, a la necesidad de encontrar un punto de equilibrio entre el libre tránsito de los datos personales a través de las fronteras y el respeto de la privacidad y las libertades individuales.[207]

1.1. Directrices de la OCDE sobre protección de la privacidad y el flujo transfronterizo de datos personales (1980)

[204] Los países miembros originales de la OCDE son Alemania, Austria, Bélgica, Canadá, Dinamarca, España, Estados Unidos, Francia, Grecia, Irlanda, Islandia, Italia, Luxemburgo, Noruega, Países Bajos, Portugal, Reino Unido, Suecia, Suiza y Turquía. Posteriormente se han adherido como miembros: Japón (1964), Finlandia (1969), Australia (1971), Nueva Zelanda (1973), México (1994), República Checa (1995), Hungría (1996), Polonia (1996), Corea (1996) y Eslovaquia (2000), Chile (2010), Eslovenia (2010), Israel (2010), Estonia (2010). La Comisión de las Comunidades Europeas participa en los trabajos de la OCDE (artículo 13 del Convenio de la OCDE).

[205] Cfr. OECD, *Annual Report*, 2009. Disponible en http://www.oecd.org/dataoecd/38/39/43125523.pdf

[206] Para mayor información sobre la OCDE, se puede consultar su página web *http://www.oecd.org*

[207] Al respecto Guerrero Picó, señala que «La protección de datos de carácter personal desde la OCDE va a ser más una exigencia en orden a facilitar las operaciones económicas entre los Estados que una necesidad derivada de la defensa de los derechos de las personas, aunque, evidentemente, redundará en beneficio de éstos», Cfr. María del Carmen, GUERRERO PICÓ, *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Thomson-Civitas, Navarra, 2006, p. 47.

1.1.1. Importancia y fundamento

La adopción de las Directrices sobre protección de la privacidad y libre flujo transfronterizo de datos personales, de 23 de septiembre de 1980, por parte del Consejo de la OCDE, se fundamenta en la constatación de la inexistencia de una uniformidad en la regulación de esta materia en los distintos Estados miembros. Al existir legislaciones con criterios dispares sobre la materia, se dificultaba el flujo de los datos personales entre los países miembros. Por ello, la finalidad principal de la Recomendación es establecer principios básicos reguladores del derecho a la privacidad que, adoptadas de forma uniforme por los Estados, garanticen la inexistencia de obstáculos a la libre transferencia internacional de datos entre aquellos.

La importancia de la Recomendación de la OCDE de 1980, radica en ser el primer documento de ámbito supranacional que analiza en profundidad el derecho a la protección de datos de carácter personal.[208] En este instrumento se establecen por primera vez, de una forma sistemática, los principios fundamentales del derecho a la protección de datos de carácter personal. Estos pasarán a constituirse «en el germen de todas las normas nacionales e internacionales sobre la materia adoptadas con posterioridad».[209] Su valor se manifiesta, también, en el hecho de ser considerado un parámetro válido de evaluación del nivel de protección otorgados por los países sobre la materia. Así lo ha manifestado el Grupo de Trabajo del artículo 29, para quien, el cumplimiento de dichos principios por parte de los Estados viene a constituir un mínimo necesario para que los mismos puedan ser considerados como oferentes de un nivel adecuado de protección de datos.[210]

El origen mediato de las Recomendaciones de la OCDE sobre la materia, lo encontramos en la década de los setenta, cuando diversos países empiezan a dictar leyes destinadas a cautelar la información personal ante el progresivo aumento de las bases de

[208] Sobre la evaluación del impacto que ha tenido las Directrices de la OCDE sobre esta materia véase: OECD (2011), «The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines», OECD Digital Economy Papers, nº. 176, OECD Publishing, *http://dx.doi.org/10.1787/5kgf09z90c31-en* [fecha consulta: 28.9.2011]

[209] Cfr. Agustín, PUENTE ESCOBAR, «Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal», en *Protección de Datos de Carácter Personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos, La Antigua – Guatemala, 2-6 de junio de 2003)*, Tirant lo Blanch, Valencia, 2006, pp. 50 y 51.

[210] Al respecto, véase el documento nº 12 del Grupo de Trabajo del artículo 29, de la Directiva 95/46/CE.

datos informatizadas. Dichas leyes, en principio, no obedecían a criterios comunes, sino que se adecuaban a las necesidades de cada país. La disparidad de criterios legislativos provocó entonces problemas al libre flujo de la información a través de las fronteras. Con la finalidad de superar dichas dificultades, la OCDE en 1976 encargó a un grupo de expertos que elaborara unas directrices.[211] Posteriormente en 1978, esta tarea será concluida por un nuevo grupo de expertos *ad hoc* sobre las barreras a los Datos Transfronterizos y la Protección de la Privacidad. A este nuevo grupo se le encargó que elaborara unas directrices sobre las normas básicas que regirían el flujo transfronterizo y la protección de los datos personales y la privacidad, para así facilitar la armonización de las diversas legislaciones nacionales sin que ello excluyera el posterior establecimiento de un convenio internacional.[212]

En los diversos borradores e informes del grupo de expertos, queda de manifiesto la especial preocupación por ciertos temas, que reseñamos a continuación:

a) *Los datos sensibles*. Se discutió la posibilidad de establecer un conjunto de datos que sean aceptados universalmente como sensibles, sin resultados positivos. Tampoco pudieron establecer un criterio rector, como sería por ejemplo el riesgo de discriminación, para definir un conjunto de datos que pudieran verse universalmente

[211] El programa de la OCDE sobre los flujos de datos transfronterizos deriva de los estudios sobre la utilización de los ordenadores en el sector público, iniciado en 1969. A partir de esta fecha un Grupo de Expertos, analizó y estudió diferentes aspectos del tema de la privacidad: la información digital, la administración pública, los flujos de datos transfronterizos y las implicaciones de las políticas en general. Estos y otros temas serán debatidos en un Simposium celebrado en Viena en 1977, en el que se recogieron opiniones y experiencias de diversos sectores (gobierno, la industria, los usuarios de redes de comunicación de datos, los servicios de proceso y organizaciones intergubernamentales interesadas). A partir de las conclusiones de dicho encuentro, se elaboraron algunos principios orientadores en un marco general de cara a una posible actuación internacional. Estos principios reconocían (a) la necesidad, en general, de flujos de información continuos e ininterrumpidos entre países, (b) los intereses legítimos de los países en evitar toda transferencia de datos que sea peligrosa para su seguridad o contraria a sus leyes sobre orden público y decencia o que viole los derechos de sus ciudadanos, (c) el valor económico de la información y la importancia de proteger el "comercio de datos" mediante normas aceptadas de leal competencia, (d) la necesidad de garantías de seguridad para minimizar las violaciones de los datos registrados y el mal uso de la información personal, y (e) la significación de un compromiso de los países para establecer un conjunto de principios fundamentales para la protección de la información personal. Cfr. los apartados 16 y 17 de la Memoria Explicativa de la Directrices de la OCDE sobre la Protección de la Privacidad y el Flujo Transfronterizo de datos personales, de 23 de septiembre de 1980.

[212] Este trabajo tenía que llevarse a cabo en estrecha cooperación con el Consejo de Europa y la Comunidad Europea y estar listo el 1º de julio de 1979. Cfr. apartado 18 de la Memoria Explicativa de la Directrices de la OCDE de 1980.

como sensibles. Ante ello, se optó por una afirmación de carácter general en el apartado 7, en el sentido de poner límites a la recogida de datos personales.[213]

b) *El Procesamiento automático de datos* (PAD, ADP en inglés). Uno de los temas más discutidos por el Grupo de Expertos, fue los problemas legales derivados de la afectación de la privacidad y las libertades individuales con el procesamiento automático de datos. Especialmente les preocupaba «el uso ubicuo de los ordenadores para procesar los datos personales, las posibilidades – mucho mayores – de almacenar, comparar, enlazar, seleccionar y acceder a los datos personales, y la combinación de los ordenadores con la tecnología de la información que permite poner los datos personales a disposición de miles de usuarios, ubicados en localidades geográficas distantes entre sí, al mismo tiempo, y permite la reunión de datos y la creación de redes complejas de datos tanto nacionales como internacionales». También centran su atención en el incipiente desarrollo de las «nuevas redes de datos internacionales, y la necesidad de equilibrar los intereses contrapuestos de privacidad por una parte y libertad de información por la otra».[214]

c) *La protección de las personas jurídicas*. Al momento de elaborar las directrices, algunas leyes nacionales protegían los datos relativos a las personas jurídicas de manera similar a como lo hacen con los datos relativos a las personas físicas. Por ello se planteó la discusión sobre si las directrices alcanzaban o no a las personas jurídicas. Algunos miembros del grupo de expertos sugirieron que se debería prever la posibilidad de ampliar las directrices a las personas jurídicas (empresas, asociaciones, etc.), pero esta postura no obtuvo el consenso necesario. Así pues, el alcance de las directrices se limita a los datos relativos a los individuos y se deja en libertad a los países miembros para decidir su extensión a las personas morales.[215]

d) *Las sanciones y los recursos*. Atendido el hecho que la OCDE la integra países con tradiciones jurídicas distintas, este punto fue abordado con suma laxitud, a objeto de reconocer la validez de los distintos sistemas jurídicos en la forma de cautelar el derecho a la privacidad de sus ciudadanos. Así tenemos, que se dan por válidas, tanto

[213] Cfr. apartados 19 a), 50 y 51 de la Memoria Explicativa.
[214] Cfr. apartados 3 y 19 b) de la Memoria Explicativa.
[215] Cfr. apartados 19 c), 31, 33 y 49 de la Memoria Explicativa.

la supervisión y control de su cumplimiento por autoridades especialmente constituidas al efecto, como aquellas que establecen el sistema de autorregulación y las que remiten a los recursos judiciales tradicionales ante sus tribunales ordinarios.[216]

e) *Los conflictos de leyes*. Ya desde la época en que se redactan estas directrices, eran particularmente complejos los temas de la elección de la jurisdicción, la ley aplicable y del reconocimiento de las sentencias extranjeras, en el contexto de los flujos de datos transfronterizos. Luego de discutir distintas estrategias y principios, sin resultados positivos, se planteó la cuestión de si debía intentarse en esta etapa proponer soluciones en las Directrices de carácter no vinculante. En definitiva no se llegó a ningún consenso sobre el punto, por lo que el tema no fue tratado en esta directriz.[217]

f) *Las excepciones al cumplimiento de la directriz.* Se discutió dentro del grupo de expertos la necesidad de establecer excepciones en la misma directriz y, en caso afirmativo, definir la forma de las mismas. Se plantearon dos posturas. Una era establecer excepciones con carácter general y, la otra, instaurar las mismas con algunos límites. Al final se optó por esta última opción, pero bajo dos condiciones: que fueran "las menos posibles" y "puestas en conocimiento del público".[218] La fórmula amplia indicada permite a los Estados establecer otros factores limitadores, diferentes de los mencionados expresamente —soberanía nacional, la seguridad nacional y el orden público—. De todas formas, queda claro que el fundamento de la limitación debe ser de tal entidad, que pueda ser considerado un «asunto nacional decisivo». A nuestro juicio la regulación es insuficiente, como lo reconoce el propio informe explicativo (apdo. 20). Por suerte, este punto será desarrollado con mayor detalle por otros instrumentos internacionales dictados con posterioridad sobre la materia, como el Convenio 108 del Consejo de Europa.[219]

g) *El problema de la preeminencia entre protección de datos y el libre flujo de los mismos.* De la simple lectura de la Memoria Explicativa de las Directrices, queda la impresión de que en aquella época se planteaba como casi imposible, o al menos de gran dificultad, tratar de conciliar los valores en juego, estos es, el respeto por la

[216] Cfr. apartados 14, 19 d) de las Directrices y los apartados 19 d) y 62 de la Memoria Explicativa.
[217] Cfr. apartado 19 f) y 74 de la Memoria Explicativa.
[218] Cfr. apartado 4 de la Directriz.
[219] Cfr. apartado 19 g), 20, 46 y 47, de la Memoria Explicativa.

privacidad y las libertades individuales, por una parte, como el libre tránsito de los datos personales a través de las fronteras, por otra. Se llega a señalar que «se debe hacer hincapié en uno o en otro, y es difícil distinguir entre los intereses de la protección de la privacidad y otros intereses relativos al comercio, la cultura, la soberanía nacional, etc.».[220]

El trabajo realizado por el grupo de expertos, dará finalmente como resultado la Recomendación del Consejo de la OCDE, aprobada el 23 de septiembre de 1980, sobre líneas directrices que han de regir en la protección de la vida privada y los flujos transfronterizos de datos de carácter personal. Estas tienen por objeto «sugerir» a los Estados miembros que tengan en cuenta las directrices en el tratamiento de datos personales tanto en el ámbito nacional como internacional (transferencia internacional de datos), con el fin de tratar de conciliar el respeto de la privacidad con el tratamiento de datos personales.[221]

Visto el contexto en que surgen la directrices, corresponde ahora dar una visión general al contenido de las mismas.

1.1.2. Estructura y contenido

El instrumento de la OCDE que regula la privacidad y la transferencia internacional de datos, se estructura con un Preámbulo, la Recomendación, un Anexo a la Recomendación que contiene las Directrices propiamente tales y que forma parte de la misma y, por último, una Memoria Explicativa.

En el Preámbulo de la Recomendación se indica que el tratamiento automatizado de datos y el libre flujo transfronterizo de los mismos, se consideran un elemento de desarrollo socioeconómico. Por ello se busca elaborar normas y prácticas compatibles entre los Estados a objeto de evitar posibles obstáculos injustificados en las

[220] Cfr. apartado 19 h) de la Memoria Explicativa.

[221] Algunos autores como Guerrero Picó, sólo ven en las directrices la finalidad de «suprimir (o, directamente, no crear) obstáculos injustificados que, en nombre de la protección a la vida privada, dificulten el flujo internacional de datos de carácter personal». Véase, María del Carmen GUERRERO PICÓ, *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Thomson-Civitas, Navarra, 2006, p. 50.

legislaciones locales de los países miembros. De esta forma se intenta conciliar el respeto a la privacidad con el libre flujo de la información, que como señalamos anteriormente en aquel tiempo se veía como dos valores contradictorios.

En la Recomendación se insta a los países miembros a tomar en cuenta en su legislación interna los principios contenidos en las directrices, a eliminar o evitar que aparezcan, en nombre de la privacidad, obstáculos injustificados para los flujos transfronterizos de datos personales y a convenir procedimientos de implementación, colaboración y cooperación para la aplicación de las directrices.

Las directrices propiamente tales que, como se señaló, están expuestas en un Anexo a la Recomendación que forma parte de la misma, constan de cinco partes. La primera contiene una serie de definiciones y en ella se especifica el objetivo de las directrices, indicando que representan «normas mínimas» (apartados 1 a 6). La segunda parte contiene ocho principios básicos relativos a la protección de la privacidad y las libertades individuales a nivel nacional (apartados 7 a 14). La tercera parte se ocupa de los principios de aplicación internacional, es decir, principios que tienen que ver sobre todo con las relaciones entre los países miembros. La cuarta parte trata, en términos generales, de los medios para poner en marcha los principios básicos expuestos en las partes anteriores y en ella se especifica que esos principios deberían aplicarse sin discriminaciones. La quinta parte se ocupa de asuntos de asistencia mutua entre los países miembros, principalmente a través del intercambio de información y evitando procedimientos nacionales incompatibles para la protección de los datos personales. Termina con una referencia a temas relativos a la ley aplicable, cuando en la transferencia de datos personales intervengan varios países miembros.

En la primera parte, se formulan sólo tres definiciones: «inspector de datos» (responsable del tratamiento), «datos personales» y «transferencia internacional de datos personales».[222] La propia Memoria Explicativa de la Recomendación reconoce que «la

[222] Guerrero Picó, califica las definiciones de "parcas", ya que sólo especifican que «controlador de datos» es una parte que, conforme a su Derecho interno, es competente para decidir acerca del contenido y uso de los datos personales, sin tener en cuenta el hecho de que tales datos sean recogidos, almacenados, procesados o divulgados por dicha parte o por un agente en nombre suyo. «Datos personales» es cualquier información relativa a una persona identificada o identificable (sujeto de datos) y «flujos transfronterizos de datos personales», movimiento de datos personales a través de fronteras

lista de definiciones se ha quedado corta» (apartado 40). Por ejemplo, falta una definición sobre "tratamiento de datos". Es probable que ello se haya debido a la imposibilidad en aquel tiempo de llegar a un consenso sobre otras definiciones universalmente aceptadas.

Sobre el alcance de la Directiva, la primera parte establece determinadas declaraciones sobre su ámbito de aplicación, a fin de que no pueda considerarse que el establecimiento de los estándares previstos en la directiva pueda implicar una reducción del respeto al derecho a la privacidad. También se indica que las directrices se aplican tanto a los sectores públicos como privado, y que las mismas constituyen un catálogo de mínimos en esta materia, al disponer el apartado 6 que las directrices «deben ser consideradas un estándar mínimo y pueden ser complementadas por medidas adicionales de protección de la privacidad y las libertades individuales».[223]

La segunda parte de la Recomendación establece los principios básicos que han de regir en la regulación nacional de los Estados miembros sobre el tratamiento de datos personales. Estos principios son: de limitación de recogida; de calidad de los datos; de especificación de los fines; de limitación de uso; de salvaguarda de la seguridad; de transparencia; de participación individual; y el principio de responsabilidad.[224]

---

nacionales. Cfr. María del Carmen, GUERRERO PICÓ, *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Thomson-Civitas, Navarra, 2006, p. 50.

[223] En el mismo sentido, véase Agustín, PUENTE ESCOBAR, «Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal», en *Protección de Datos de Carácter Personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos, La Antigua – Guatemala, 2-6 de junio de 2003)*, Tirant lo Blanch, Valencia, 2006, p. 52.

[224] Para un mayor desarrollo de los mismos, véase los apartados 50 a 62 de la Memoria Explicativa. Siguiendo a Puente Escobar, podemos reagrupar los 14 principios enunciados en 7, de la siguiente forma: los datos deben ser recogidos y tratados de forma leal y lícita, recabándose previamente el consentimiento del interesado, o al menos informando al mismo de esa recogida; el responsable del tratamiento deberá especificar la finalidad para la que trata los datos, no pudiendo utilizar los mismos para un fin incompatible con la finalidad declarada; los datos sometidos a tratamiento deben ser adecuados, pertinentes y no excesivos en relación con la finalidad declarada; el responsable del tratamiento deberá adoptar las medidas de seguridad en el tratamiento, necesarias para evitar la pérdida o acceso no autorizado a los datos; el responsable del tratamiento deberá informar a los afectados acerca del tratamiento de sus datos de carácter personal que se proponga realizar; los afectados tienen derecho a conocer la existencia de un tratamiento de sus datos de carácter personal; los afectados tienen derecho a solicitar, en su caso, la rectificación o cancelación de sus datos sometidos a tratamiento. Cfr. Agustín, PUENTE ESCOBAR, «Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal», en *Protección de Datos de Carácter Personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos, La Antigua – Guatemala, 2-6 de junio de 2003)*, Tirant lo Blanch, Valencia, 2006, pp.52 y 53.

La tercera parte de la Recomendación se centra en los principios básicos que deben regir en la transferencia internacional de datos personales, a objeto de garantizar el libre flujo de los mismos. El principio básico que rige la materia es que todo Estados miembro debe garantizar la seguridad del tráfico de la información (apartado 16). No obstante, como condición previa, las directrices exigen que el Estado de destino observe sustancialmente las directrices (apartado 17). Además, se permite a los países miembros establecerse restricciones adicionales en relación con ciertas categorías de datos para los que la ley nacional establezca reglas especiales en atención a su naturaleza, si el Estado de destino no ofrece un nivel de protección equivalente. Dichas restricciones deben ser proporcionadas en relación a los fines perseguidos por la misma (apartado 17, parte final y 18).

Por último, los apartados cuarto y quinto regulan las medidas de implantación de las directrices y la cooperación entre los Estados miembros. En cuanto a las medidas de implantación de las directrices, se indica el deber de los Estados miembros de establecer medidas legales, administrativas de otra índole para la protección de la privacidad y las libertades individuales en relación con los datos personales. En particular, las directrices se refieren a la adopción de normas nacionales y al fomento de la autorregulación y la adopción de códigos de conducta (apartado 19).[225] Como se puede apreciar, la normativa deja a cada Estado buscar los mecanismos por los cuales implementará las directrices, sin imponer la creación de un órgano destinado particularmente al efecto.

1.2. Otras Recomendaciones de la OCDE vinculadas a la privacidad

Desde que la OCDE aprobó en 1980 las Directrices sobre Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales, el desarrollo tecnológico en diversas áreas y, particularmente, en los sistemas y redes de información y comunicación han sufrido grandes cambios. No obstante, el carácter «neutral» desde el punto de vista tecnológico de las directrices, ha permitido que sus principios continúen representando un consenso internacional y una orientación en cuanto a la recogida y

[225] Agustín, PUENTE ESCOBAR, «Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal», en *Protección de Datos de Carácter Personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos, La Antigua – Guatemala, 2-6 de junio de 2003)*, Tirant lo Blanch, Valencia, 2006, p. 53.

manejo de datos personales, realizado por cualquier medio o soporte, proporcionando la base para la protección de la privacidad en todo tipo de tratamiento. Es por ello, que las nuevas Directrices de la organización que se vinculan a temas de privacidad y protección de datos personales, señalan que han de ser interpretadas a la luz de aquella.[226]

En la década de los 90', la OCDE desarrolló directrices a seguir en diversos ámbito vinculados a la privacidad, tales como: la Recomendación relativa a la seguridad de los sistemas de información, 26 de noviembre de 1992; la Recomendación relativa a las directrices de política criptográfica, adoptada por el Consejo de la OCDE, de 27 de marzo de 1997; la Declaración Ministerial sobre Protección de la Privacidad en las Redes Globales y la Declaración Ministerial sobre la Autentificación del Comercio Electrónico, ambas de diciembre de 1998. Estos instrumentos tienen como elemento común, el compromiso de los Estados Miembros con el respeto al derecho a la privacidad, la necesidad de generar confianza en las nuevas tecnologías y evitar restricciones innecesarias en los flujos transfronterizos de datos personales.[227]

A principios de este siglo, producto de los atentados a Estados Unidos, el Comité de Política de la Información, de la Informática y de las Comunicaciones de la OCDE, encargó la revisión de las Directrices sobre seguridad de 1992 (reexaminadas en 1997) al Grupo de expertos de Seguridad de la Información y Protección de la Privacidad.[228] Como resultado de este estudio, acelerado por la tragedia del 11 de septiembre, el Consejo de la OCDE adopta en 2002 esta nueva Recomendación que

[226] En el mismo sentido, véase la Declaración relativa a los flujos de datos transfronterizos, adoptada por los Gobiernos de los países Miembros de la OCDE, el 11 de abril de 1985 y las *Directrices de la OCDE para la Seguridad de Sistemas y Redes de Información: hacia una cultura de Seguridad*, de 25 de julio de 2002, nota a pie de pág. nº 1, p. 6.

[227] Cfr. *Resumen de las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales*, OCDE, 2002, p 3. Disponible en línea en: www.oecd.org/bookshop. [fecha consulta: 29.9.2011]

[228] Este Grupo de Trabajo de la OCDE sobre la Seguridad de la Información y Privacidad (conocido por su sigla inglesa: *WPISP*) ha desarrolla trabajos en diversas áreas, tales como: Infraestructura de información crítica (CII), gestión de identidad digital (IDM) y la autenticación electrónicas, malware, identificación por radiofrecuencia (RFID), redes de sensores, las Directrices de Privacidad de la OCDE y la protección de los niños en línea. Para mayor información, véase *http://www.oecd.org/document/46/0,3343,en_2649_34255_36862382_1_1_1_1,00.html*

reemplaza a la anterior y regula las líneas directrices en lo referente a la seguridad de los sistemas y redes de información.[229]

Estas nuevas Directrices sobre seguridad, están dirigidas tanto a los países miembros como aquellos que no forman parte de la organización, del sector público y privado. Busca promover una cultura de seguridad y hacer que todas las partes involucradas asuman su responsabilidad en la materia, adoptando las medidas oportunas para ejecutar estas Directrices. También exhorta a establecer nuevas políticas, prácticas, medidas y procedimientos, que se examinaran cada cinco años, a objeto de adoptar y promover una cultura de la seguridad a nivel internacional. Cabe destacar, que las medidas para fortalecer la seguridad de los sistemas y redes de información «deben ser consistentes con los valores de una sociedad democrática, en particular con la necesidad de contar con flujos de información libres y abiertos, y los principios básicos de protección de la privacidad personal».[230]

[229] Guerrero Picó menciona los siguientes documentos: DSTI/ICCP/REG(2002)6FINAL, de 21/01/2003, que muestran el plan de puesta en marcha de dichas directrices y el DSTI/ICCP/REF(2005)1/FINAL, de 16/12/2005, que da cuenta de cómo han comenzado a implantarse. Cfr. María del Carmen, GUERRERO PICÓ, *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Thomson-Civitas, Navarra, 2006.p. 53.

[230] Los principios que recoge la Directiva sobre Seguridad de Sistemas y Redes de Información, son los siguientes: 1) *Sensibilización*: Los Estado miembros de la OCDE deben tomar conciencia de la necesidad de asegurar la seguridad de los sistemas y redes de información. 2) *Responsabilidad:* Las Partes son responsables de la seguridad de los sistemas y redes de información. Han de comprender su parte de responsabilidad en lo que concierne a estas rede locales y mundiales (interconectadas) y examinar y evaluar regularmente sus políticas en este ámbito para asegurarse de su adaptación al entorno. 3) *Reacción:* Actuarán con prontitud y espíritu de cooperación para prevenir, detectar y responder a los incidentes de seguridad, intercambiando para ello las informaciones que posean sobre vulnerabilidades y amenazas. 4) *Ética:* Respetarán, a su vez, los intereses legítimos de las otras Partes, teniendo en cuenta si su actividad o la ausencia de ésta les puede causar algún perjuicio y adoptando prácticas ejemplares. 5) *Democracia:* La seguridad de los sistemas y redes de información tiene que ser compatible con los valores fundamentales de una sociedad democrática, especialmente con la libertad de expresión, la libre circulación de la información y de las comunicaciones, la protección adecuada de los datos personales, la apertura y la transparencia. 6) *Evaluación de los riesgos*: Las Partes evaluarán los riesgos y, tomando en consideración la naturaleza y relevancia de la información a proteger, los perjuicios a los intereses de otros, etc., seleccionaran las medidas de control oportunas. 7) *Concepción y puesta en marcha de la seguridad:* Han de integrar la seguridad (con medidas técnicas y no técnicas) como una pieza esencial a optimizar en la arquitectura de los sistemas y redes de información. 8) *Gestión de la seguridad:* Los Estados adoptarán un enfoque global de la gestión de la seguridad, una evaluación dinámica de los riesgos que cubran todos los niveles de actividad de las partes intervinientes y todos los aspectos de sus operaciones. Asimismo deberán incluir, por anticipación, respuestas a las amenazas emergentes y cubrir la prevención, detección y resolución de incidentes, la recuperación de los sistemas, el mantenimiento permanente, el control y la auditoria. 9) *Reevaluación.* Las Partes deben examinar y reevaluar la seguridad de los sistemas y redes de información e introducir las modificaciones apropiadas a sus políticas, prácticas, medidas y procedimientos de seguridad. Cfr. el Título III (Principios), de las *Directrices de la OCDE para la Seguridad de Sistemas y Redes de Información*, pp. 6-8.

Otro instrumento importante adoptado por la OCDE, de 12 de junio de 2007, es la Recomendación relativa a la cooperación transfronteriza en la aplicación de las legislaciones que protegen la privacidad, que pretende optimizar los marcos normativos nacionales para una mejor aplicación de las leyes sobre privacidad. Se busca, principalmente, permitir que las autoridades nacionales puedan cooperar más eficazmente con autoridades de terceros países y que se puedan elaborar mecanismos internacionales eficaces que faciliten la cooperación internacional en la aplicación de las leyes de privacidad.

Como hemos podido apreciar, los principios establecidos en las directrices de privacidad de la OCDE, se caracterizan por su amplitud y flexibilidad. Ello le ha permitido adaptarse a los cambios tecnológicos, al ser capaz de abarcar «todos los medios del procesamiento informático de datos sobre individuos (desde computadoras locales a redes con complejas ramificaciones nacionales e internacionales), a todos los tipos de procesamiento de datos personales (desde la administración de personal hasta la compilación de perfiles de consumidores) y todas las categorías de datos (desde datos de tráfico hasta datos de contenidos, desde el más trivial al más delicado)». Asimismo, sus principios se pueden aplicar tanto en el ámbito nacional como internacional.[231]

2. DIRECTRICES DE LA ONU PARA LA REGULACIÓN DE LOS ARCHIVOS DE DATOS PERSONALES INFORMATIZADOS

En 1990, la Asamblea General de las Naciones Unidas, adoptó las Directrices para la Regulación de los Archivos de Datos Personales Informatizados.[232] Su importancia radica en que contiene una lista mínima de principios que debería ser adoptados tanto por las legislaciones internas de todos sus Estados miembros, como por las Organizaciones Internacionales Gubernamentales (en adelante, OIG)[233] constituyendo así, el primer documento de ámbito universal en la materia.

---

[231] *Resumen de las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales*, OCDE, 2002, pp. 2 y 3. Disponible en línea en: *www.oecd.org/bookshop* [fecha consulta: 29.9.2011]

[232] Resolución 45/95 de la Asamblea General de las Naciones Unidas, de 14 de diciembre de 1990.

[233] Michel Virally, define a las Organizaciones Internacionales Gubernamentales como «una asociación de Estados, establecida por un acuerdo entre sus miembros y dotada de un aparato permanente de órganos, encargado de perseguir la realización de objetivos de interés común por medio de una cooperación entre ellos». Citado por CALDUCH CERVERA, Rafael, *Relaciones Internacionales*,

Al igual que ocurre con las Directrices de la OCDE, carecen de fuerza obligatoria vinculante para los Estados miembros. Por tanto, su contenido constituye básicamente «orientaciones» para llevar a la práctica las normas relativas a los archivos de datos personales informatizados. Es un texto sumamente breve, dividido en dos partes. En la primera (A), contiene los principios básicos de protección de datos, y en la segunda (B), la aplicación de las Directrices a los tratamientos llevados a cabo por las OIG.

Los principios básicos, cuya implementación se deja a iniciativa de cada Estado, son los siguientes:

- *Principio de legalidad y lealtad.* La información relativa a las personas no debe ser recogida o procesada por métodos desleales o ilegales, ni debe ser utilizada para fines contrarios a los fines y principios de la Carta de Naciones Unidas.

- *Principio de exactitud.* Las personas responsables de la compilación de archivos, o aquellas responsables de mantenerlos, tienen la obligación de llevar a cabo comprobaciones periódicas acerca de la exactitud y pertinencia de los datos registrados y garantizar que los mismos se mantengan de la forma más completa posible, con el fin de evitar errores de omisión, así como de actualizarlos periódicamente o cuando se use la información contenida en un archivo, mientras están siendo procesados.

- *Principio de finalidad*. La finalidad a la que vaya a servir un archivo y su utilización en términos de dicha finalidad debe ser especificada, legítima y, una vez establecida, recibir una determinada cantidad de publicidad o ser puesta en conocimiento de la persona interesada, con el fin de que posteriormente sea posible garantizar que: a) todos los datos personales recogidos y registrados sigan siendo pertinentes y adecuados para los fines especificados; b) ninguno de los referidos datos personales sea utilizado o revelado, salvo con el consentimiento de la persona afectada, para fines incompatibles con aquellos especificados; c) El período durante el que se

Ediciones Ciencias Sociales. Madrid, 1991, http://www.ucm.es/info/sdrelint/ficheros_aula/aula1405.pdf [consulta 29.9.2011].

guarden los datos personales no supere aquel que permita la consecución de los fines especificados.

- *Principio de acceso de la persona interesada*. Cualquiera que ofrezca prueba de su identidad tiene derecho a saber si está siendo procesada información que le concierna y a obtenerla de forma inteligible, sin costes o retrasos indebidos; y a conseguir que se realicen las rectificaciones o supresiones procedentes en caso de anotaciones ilegales, innecesarias o inexactas, y, cuando sea comunicada, a ser informado de sus destinatarios. Debe preverse un recurso, en caso necesario, ante la autoridad supervisora correspondiente. El coste de cualquier rectificación será soportado por la persona responsable del archivo. Es conveniente que las disposiciones relacionadas con este principio se apliquen a todas las personas, sea cual sea su nacionalidad o lugar de residencia.

- *Principio de no discriminación*. Sin perjuicio de los casos susceptibles de excepción restrictivamente contemplados en el siguiente principio, no deben ser recogidos datos que puedan dar origen a una discriminación ilegal o arbitraria, incluida la información relativa a origen racial o étnico, color, vida sexual, opiniones políticas, religiosas, filosóficas y otras creencias, así como la circunstancia de ser miembro de una asociación o sindicato.

- *Facultad para hacer excepciones.* Las excepciones a los cuatro primeros principios señalados solamente pueden ser autorizadas en caso de que sean necesarias para proteger la seguridad nacional, el orden público, la salud pública o la moralidad, así como, entre otras cosas, los derechos y libertades de otros, especialmente de personas que estén perseguidas (cláusula humanitaria). Tales excepciones deben estar especificadas de forma explícita en una ley o norma equivalente promulgada de acuerdo con el sistema jurídico interno, que expresamente establezca sus límites y prevea las salvaguardas adecuadas. Las excepciones al principio relativo a la prohibición de la discriminación, además de estar sujetas a las mismas salvaguardas que las prescritas para las excepciones a los principios 1 a 4, solamente podrán autorizarse dentro de los límites establecidos en la Carta Internacional de Derechos Humanos y en el resto de instrumentos aplicables en el campo de la protección de los Derechos Humanos y la prevención de la discriminación.

- *Principio de seguridad*. Deben adoptarse medidas adecuadas para proteger los archivos, tanto contra peligros naturales, la pérdida o destrucción accidental, como también de actos humanos, como el acceso no autorizado, el uso fraudulento de los datos o la contaminación mediante virus informáticos.

Respecto del cumplimiento de las Directrices, se establecen que el derecho de cada país designará a la autoridad que, de acuerdo con su sistema jurídico interno, vaya a ser responsable de supervisar la observancia de los principios arriba establecidos. Esta autoridad debe ofrecer garantías de imparcialidad e independencia frente a las personas o agencias responsables de procesar y establecer los datos, y competencia técnica.

En caso de violación de lo dispuesto en la ley nacional que lleve a la práctica los principios anteriormente mencionados, deben contemplarse condenas penales u otras sanciones, junto con los recursos individuales adecuados.

Sobre las transferencias internacionales de datos personales, las directrices señalan 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.

Respecto de su ámbito o campo de aplicación, se dispone que los presentes principios se aplican, en primer lugar, a todos los archivos informatizados públicos y privados, así como, mediante extensión optativa y sujeta a los ajustes correspondientes, a los archivos manuales. Pueden dictarse disposiciones especiales, también optativas, para hacer aplicable la totalidad o parte de los principios a los archivos relativos a personas jurídicas, especialmente cuando contengan alguna información relativa a individuos.

La segunda parte de las directrices de la ONU, se refiere a los archivos de datos personales informatizados mantenidos por Organizaciones Internacionales

Gubernamentales en adelante (OIG)[234], sea para fines internos —aquellos que conciernen a la gestión de personal— o para fines externos —relativos a terceros que tengan relaciones con la organización—. Cada organización debe designar a la autoridad legalmente competente para supervisar la observancia de estas directrices. Al respecto, Estadella, ha señalado que «con ello se evita que la función de control sea una más de los órganos existentes, resaltándose la importancia de la autoridad y protegiéndose la efectividad de la normativa sobre protección de datos».[235]

Por último, en las Directrices se contempla una "cláusula humanitaria" de exclusión o excepción de aplicación de estos principios en determinados supuestos: cuando la finalidad del archivo sea la protección de los Derechos Humanos y las libertades fundamentales de la persona afectada o la ayuda humanitaria. También debe preverse una excepción similar en la legislación nacional a favor de las OIG.

3. FORO DE COOPERACIÓN ECONÓMICA ASIA-PACÍFICO (APEC)

El Foro de Cooperación Económica Asia Pacífico (en adelante, APEC), fue creado en 1989, como un instrumento de cooperación económica y técnica para facilitar el comercio y las inversiones regional de los países miembros en territorios de la cuenca del Océano Pacífico.[236]

La APEC no posee un tratado formal, por tanto, sus decisiones se deben toman por consenso y sus declaraciones no son vinculantes para los países miembros. No obstante, sus acuerdos y declaraciones sirven de guía a los países miembros en cuanto a las políticas normativas a seguir en los diferentes tópicos vinculados a sus objetivos.

---

[234] Para una mayor profundización sobre este tipo de organizaciones, véase CALDUCH R., *Relaciones Internacionales***,** Ediciones Ciencias Sociales. Madrid, 1991, *http://www.ucm.es/info/sdrelint/ficheros_aula/aula1405.pdf»* [consulta 29.9.2001]

[235] Olga ESTADELLA YUSTE, *"La protección de la intimidad frente a la transmisión internacional de datos personales"*, Ed. Tecnos, Madrid, 1995, págs. 144 y 145.

[236] La suma del Producto Nacional Bruto de las 21 economías que conforman el APEC equivale al 56 por ciento de la producción mundial, en tanto que en su conjunto representan el 46 por ciento del comercio global. Actualmente, son Países Miembros de la APEC: Australia (1989), Brunéi (1989), Canadá (1989), Indonesia (1989), Japón (1989), Corea del Sur (1989), Malasia (1989), Nueva Zelanda (1989), Filipinas (1989), Singapur (1989), Tailandia (1989), Estados Unidos (1989), China Taipéi (1991), Hong Kong China (1991), República Popular China (1991), México (1993), Papúa Nueva Guinea (1993), Chile (1994), Perú (1998), Rusia (1998), Vietnam (1998). Para mayor detalle sobre la organización, véase *http://www.apec.org*

Uno de estos fines es el vinculado al comercio electrónico y la protección de datos.[237] La APEC se percató que una parte importante de los esfuerzos para mejorar la confianza de los consumidores y garantizar el crecimiento del comercio electrónico, se debe focalizar en el establecimiento de estándares mínimos para la protección efectiva de privacidad. De esta forma, se favorece el libre flujo de la información personal en toda la región Asia-Pacífico, lo que redunda en una mejora en los negocios transfronterizos.

3.1. Marco de Privacidad de 2004

En noviembre de 2004, la APEC aprobó su "Marco de Privacidad" (*APEC Privacy Framework*), con el ánimo de fortalecer la protección de la privacidad y permitir los flujos internacionales de información.[238] Este documento, se estructura en cuatro partes. La primera parte, contiene un preámbulo de carácter introductorio; en la segunda parte, se determina su ámbito de aplicación; la parte tercera, se destina a los principios; y la última, da reglas para la implementación tanto a nivel nacional como internacional de los principios.

El preámbulo deja claro la visión economicista de la necesidad de regular el tema, al enmarcar la regulación de la privacidad dentro de un plan de acción que pretende el desarrollo del comercio electrónico. La APEC razona sobre la base que «la falta de confianza del consumidor en la privacidad y seguridad de las transacciones en línea y redes de información es un elemento que puede impedir que las economías miembros obtengan todos los beneficios del comercio electrónico».[239] Por tanto, a mayor respeto por la privacidad, mayor será la confianza de los consumidores, lo que redundará en un aumento del comercio electrónico. Es evidente entonces que la búsqueda de una mayor protección de los derechos y libertades de los ciudadanos de los

---

[237] Véase: *http://www.apec.org/Home/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group*

[238] Este objetivo queda claro al contrastar su Declaración: «*Ministers have endorsed the APEC Privacy Framework, recognizing the importance of the development of effective privacy protections that avoid barriers to information flows, ensure continued trade, and economic growth in the APEC region*». Cfr. APEC Secretariat, «*APEC Privacy Framework*», 2005, p. 1, Disponible en línea en *http://publications.apec.org/publication-detail.php?pub_id=390*

[239] Cfr. APEC Secretariat, «*APEC Privacy Framework*», 2005, p. 2.

países miembros de la APEC, no es aliciente principal para regular el tratamiento de datos personales. Nuevamente, como en el caso de la OCDE, la protección de la privacidad será una consecuencia *accesoria* de la necesidad de eliminar las "barreras" al libre comercio.

En la segunda parte, se determina el alcance o ámbito de los principios contenidos en este Marco de Privacidad de la APEC. En cuanto a los sujetos, se establece que sólo se aplica a las informaciones personales de las personas físicas. Se entiende por «información personal» la información que se puede utilizar para identificar a un individuo, o lo haga identificable. Esto último, implica información que por sí solo no permite la identificación del individuo, pero que puestos en relación con otra, puede permitir la identificar la persona.[240] Quedan excluidas de esta regulación, el tratamiento de datos de las personas jurídicas.[241] También, queda excluida: la información recolectada y utilizada con fines exclusivamente domésticos; las que voluntariamente las personas colocan a disposición del público; los documentos oficiales que se encuentren a disposición pública; los informes periodísticos, y la información requerida por la ley para ser puesta a disposición de todos.[242] Las tres últimas hipótesis de exclusión descritas son sumamente amplias, por lo que podría dar lugar a posibles abusos si no se toman los resguardos necesarios. Por ello, es preciso, que las legislaciones nacionales que las contemplen recurran a criterios de habilitación legal, basados en los principios de finalidad y proporcionalidad.

Para la elaboración de la tercera parte del documento, dedicada a los principios, la APEC ha tomado en cuenta los principios de protección de la privacidad y el flujo transfronterizo de datos de la OCDE. Los podemos sintetizar, de la siguiente forma:

[240] Cfr. APEC Secretariat, «*APEC Privacy Framework*», 2005, p. 5.
[241] También se define al responsable del tratamiento, como «Controlador de la información personal», entendiendo por tal «una persona u organización que controla la recolección, posesión, elaboración o empleo de personal de la información. Incluye una persona o organización que da instrucciones a otra persona u organización para recolectar, mantener, procesar, utilizar, transferir o revelar información personal sobre su nombre, pero no incluye una persona u organización que lleva a cabo funciones tales como instruido por otra persona o la organización. También se excluye una persona que recoja, posea, los procesos o el uso personal información en relación con la personal de un individuo, familia o asuntos del hogar». Cfr. APEC Secretariat, «*APEC Privacy Framework*», 2005, p. 6.
[242] Cfr. APEC Secretariat, «*APEC Privacy Framework*», 2005, pp. 6-7.

- *Principio de prevención de daños*: busca evitar el mal uso de datos al momento de la recogida, uso y cesión de la información personal. Incluye dentro de estas medidas tanto la autorregulación, la educación y campañas de sensibilización, como la adopción de leyes, reglamentos y mecanismos de aplicación. Estas prevenciones, deben ser proporcionadas a la probabilidad y severidad de la amenaza de daño.[243]

- *Principio de información previa (conocimiento)*: se debe informar al titular sobre las políticas de manejo de sus datos. Se impone la obligación al controlador de la información personal (responsable del fichero) de proporcionar información clara y accesible sobre sus prácticas y políticas con respecto a la información personal, la que debe incluir: a) el hecho de que la información personal es recolectada; b) los fines para los que se recoge la información personal; c) los tipos de personas u organizaciones a las que la información personal puede ser divulgada; d) la identidad y la ubicación del controlador de información personal, incluyendo información sobre cómo contactar con ellos acerca para informarse de sus prácticas y manejo de información personal; e) las opciones, lo cual significa que el controlador ofrezca a las personas afectadas la información personal, para limitar el uso y la divulgación de sus datos, y para tener acceso y corregir su información personal.[244]

- *Principio de limitación a la recolección*: los datos se deben recabar por medios legales y justos, con el consentimiento del individuo. La recopilación de información personal debe ser limitada a la información que es pertinente a los fines de la recogida. Dicha información debe ser obtenida por medios legítimos y justos, y en su caso, con conocimiento o consentimiento de la persona en cuestión.[245]

- *Principio de uso de información personal (finalidad)*: los datos recabados deben usarse para cumplir el propósito de la recolección. Excepcionalmente, se permite el uso de los datos para otros fines diferentes de los originales: cuando exista consentimiento de la persona cuya información personal sea recogida; cuando sea necesario para proporcionar un servicio o producto solicitado por el mismo individuo; o cuando la ley u otros instrumentos jurídicos lo ordenen. El criterio fundamental que se

[243] Cfr. apartado 14 del Marco de Privacidad de la APEC, p. 11.
[244] Cfr. apartados 15 a 17, del Marco de Privacidad de la APEC, pp. 12-14.
[245] Cfr. apartado 18, del Marco de Privacidad de la APEC, p. 15.

utiliza para determinar si el propósito es compatible o relacionado con el declarado en los fines, es si el uso extendido «deriva de» o es «en cumplimiento de» tales propósitos.[246]

- *Principio de elección (información)*: persigue brindarle al titular de los datos la opción de decidir en torno a la recolección, uso y transferencia de los datos. Para ello, es necesario contar con mecanismos claros, accesibles y asequibles para el ejercicio de sus derechos. Se exime de esta obligación al responsable del tratamiento, cuando la recogida de información se ha realizado de fuentes accesibles al público.[247]

- *Principio de integridad de la información personal (calidad):* la información debe ser exacta, completa y actualizada. Para ello, el controlador de la información personal (responsable del tratamiento) está obligado a mantener la exactitud e integridad de los registros y mantenerlos al día. No obstante, se modera la intensidad del principio, al señalar en la explicación que «estas obligaciones sólo son necesarias en la medida que diga directa relación con su uso».[248]

- *Principio de seguridad:* los responsables de los ficheros, deben adoptar las medidas de seguridad apropiadas para evitar riesgos, tales como pérdida o acceso no autorizado a información personal, la destrucción no autorizada, el uso, modificación o divulgación de información. Esas salvaguardias deben ser proporcionadas a la probabilidad y la gravedad de la amenaza de daño, la sensibilidad de la información y el contexto en el que se lleva a cabo, y deben ser objeto de revisión periódica y la reevaluación.[249]

- *Principio de acceso y rectificación*: que existan mecanismos que le garanticen al titular los derechos de acceso y corrección. Este principio, le reconoce a las personas titulares de los datos, el derecho: a) a obtener la confirmación si un tercero posee información personal sobre ellos; b) que le sea comunicada en un plazo y de manera razonable, sin costos excesivos y en una forma que sea comprensible; y c) a solicitar, si procede, la rectificación, modificación o cancelación de sus datos personales.

[246] Cfr. apartado 19, del Marco de Privacidad de la APEC, pp. 16 y 17.
[247] Cfr. apartado 20, del Marco de Privacidad de la APEC, pp. 18 y 19.
[248] Cfr. apartado 21, del Marco de Privacidad de la APEC, pp. 20 y 21.
[249] Cfr. apartado 22, del Marco de Privacidad de la APEC, p. 21.

- *Principio de responsabilidad*: este principio persigue que el responsable del tratamiento actué con diligencia en el manejo de datos. Para ello, se exige que cumpla con las medidas para dar efectividad a los principios antes mencionados. Cuando la información personal deba ser transferida a otra persona u organización, ya sea nacional o internacionalmente, el controlador de información personal debe obtener el consentimiento de la persona o actuar diligentemente y tomar las medidas razonables para asegurarse de que la persona u organización receptora proteja la información de forma consistente con estos principios.[250] Lo señalado en esta última parte hay que analizarlo con cautela, ya que implicaría que el exportador de datos podría actuar sin el conocimiento y/o consentimiento de la persona afectada, siempre y cuando actúe «diligentemente» y adopte «medidas razonables de seguridad». El problema radica en quien califica cuando se actúa de tal manera. De esta forma, sería recomendable exigir, por una parte, al menos el conocimiento de la persona afectada y, por otra, que para dicha transferencia de datos exista un nivel adecuado de protección por parte del sujeto que los recibe para su tratamiento.

Estos principios consagrados en el Marco de Privacidad de la APEC son sumamente amplios y flexibles en su aplicación por parte de cada Estado miembros, lo que se justifica en el propio documentos en virtud de las diferencias sociales, culturales, económicas y jurídicas de los miembros, lo que exige flexibilidad en la aplicación de estos principios.[251]

Por último, las excepciones al cumplimiento de estos principios, incluyen las relacionadas con la soberanía, la seguridad nacional, seguridad pública y la política pública. Estas excepciones, debe ser: a) limitadas y proporcionadas al cumplimiento de los objetivos que persiguen y b) con conocimiento del público y de conformidad con la ley.[252]

[250] Cfr. apartado 26, del Marco de Privacidad de la APEC, pp. 28-30.
[251] Cfr. apartado 12, del Marco de Privacidad de la APEC, p. 7.
[252] Cfr. apartado 13 del Marco de Privacidad de la APEC, p. 8.

3.2. Reglas de privacidad transfronteriza (2007)

En septiembre de 2007, los ministros de la APEC alcanzaron el acuerdo, denominado «*Privacy Pathfinder*», para trabajar juntos en el desarrollo un sistema que prevé la mejora de las transmisiones transfronterizas de datos. [253] Para lograr dicho objetivo, se busca impulsar la aprobación de normativas que permitan esclarecer responsabilidades en los flujos internacionales de datos derivados de las necesidades empresariales, reducir los costes de cumplimiento con la normativa, facilitar a los consumidores instrumentos efectivos de protección de sus derechos, dotar de mayor eficacia a los reguladores y minimizar las cargas administrativas.[254]

Para facilitar los flujos transfronterizo de información dentro de un sistema que garantice una supervisión creíble, se promueve el uso de las «reglas de privacidad transfronterizas» (*Crossborder Privacy Rules,* en adelante CBPR). El *Pathfinder* implementa este compromiso permitiéndoles a las empresas crear y desarrollar sus propios CBPR. Las reglas de privacidad transfronteriza son acuerdos de autorregulación sobre privacidad, entre empresas de la misma área o familia. Buscan normalizar el tratamiento de datos personales, en todas sus fases, desde que los datos son recabados hasta la transmisión y posterior utilización en otros países. Para su elaboración, se toman en cuenta distintos factores, como la legislación local, los principios del Marco de Privacidad de APEC, la existencia de autoridades, sus atribuciones y ámbitos de aplicación (por ejemplo, el tipo de medidas preventivas, correctivas o sancionadoras de cada autoridad).

[253] Aprobado por los Ministros de la APEC en su reunión en Sídney, Australia en septiembre de 2007. Cabe tener presente que la búsqueda de una mejora en el tráfico transfronterizo de de datos personales, ya se podía vislumbrar en 1999, con la creación del Grupo Directivo de Comercio Electrónico (ECSG). Dicho grupo coordina actividades de promoción del comercio electrónico a través de regulaciones y políticas claras, transparentes y consistentes. Sus actividades se desarrollan en dos subgrupos: El Subgrupo de Privacidad de Datos y el Subgrupo de Comercio sin Papel. El Subgrupo de Privacidad de Datos, fue creado en 2003 y tiene como objeto principal analizar e identificar mejores prácticas en materia de privacidad y protección de datos. Entre sus principales proyectos se encuentran la promoción de la utilización de sellos de confianza (*trust marks*); la certificación, por parte de terceros, acerca de prácticas comerciales electrónicas seguras por las empresas; la elaboración de reglas de privacidad transfronteriza (*Crossborder Privacy Rules, CBPR's*) y el Proyecto explorador (*Pathfinder*).

[254] Cfr. *APEC Data Privacy Pathfinder Projects Implementation Work Plan*, 2008/SOM1/ECSG/024. Adoptado en la 17 Reunión del Grupo Directivo de Comercio Electrónico, en Lima, Perú el 24 de febrero 2008.

Para conseguir que los consumidores confíen en el sistema, se crea la figura de los «Agentes de vigilancia» (*Accountability agents*). Estos son organizaciones públicas o privadas que desempeñan una o ambas de las siguientes funciones: certifican que las CBPR de las empresas se apegan al Marco de Privacidad APEC y proporcionan servicios de resolución de conflictos en materia de privacidad entre consumidores y empresas (arbitraje). Estos agentes pueden ser la propia autoridad reguladora de la protección de datos, como por ejemplo, un comisionado de privacidad, o bien, autoridades sectoriales como las relativas a la protección del consumidor.

Otro acuerdo de la APEC vinculado a la protección de datos, se suscribió en julio de 2010. El "Acuerdo de Aplicación Transfronterizo de Privacidad" (*Cross-Border Privacy Enforcement Arrangement*, CPEA).[255] Este Acuerdo busca compartir información y proporcionar asistencia para la aplicación transfronteriza de privacidad de datos, constituyendo un paso importante en la aplicación efectiva del Marco de Privacidad de APEC.

Por último, cabe mencionar una serie de seminarios que han tenido lugar desde el 2009 en adelante, donde se han discutido temas vinculados a la protección de datos, tales como la evolución en el tratamiento de las cuestiones transfronterizas de privacidad, las marcas de confianza, los modelos de regulación, la rendición de cuentas y la privacidad, así como los problemas operativos y de gobernanza vinculados a la materia.[256]

4. NECESIDAD DE UN INSTRUMENTO JURÍDICO UNIVERSAL Y VINCULANTE

4.1. Justificación

La necesidad de un instrumentos jurídico universal y vinculante sobre el derecho fundamental a la protección de datos personales se justifica por varias razones. En

[255] Cfr. *http://apec.org/Home/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group* [fecha consulta: 7.10.2011]

[256] Estos seminarios se celebraron en Singapur en febrero y julio de 2009, en Hiroshima y Sendai, Japón, en febrero y septiembre de 2010, y en Washington DC, Estados Unidos en marzo de 2011.

primer lugar, como lo hemos adelantado al inicio de este apartado, aún persisten grandes diferencias entre los marcos normativos de los diversos países alrededor del mundo sobre la forma en que se regula la privacidad. [257] Más aún, existen Estados que carecen de normativa alguna sobre la materia y otros que, poseyéndola, no ofrecen un nivel adecuado o satisfactorio de protección. Por otra parte, hemos transitado desde la macro-informática, pasando por la micro-informática, hasta llegar a la era de Internet, los grandes buscadores y el uso extendido de redes sociales. En esta nueva realidad, el derecho a la protección de datos y el respeto a la privacidad es una condición indispensable para el desarrollo de la persona en una sociedad libre y democrática. En definitiva, «la protección de la privacidad en un entorno globalizado sólo es posible si se consensuan unas normas de protección de datos personales —asumiendo que existen visiones diferentes en los distintos continentes— y si éstas se extienden a todos los países».[258]

Como hemos visto en los apartados anteriores, diversas organizaciones, como la OCDE, APEC y ONU han intentado dar pautas para regular y conciliar el derecho a la privacidad y protección de datos personales con el libre tráfico de la información, propio de la sociedad de mercado en la que nos encontramos insertos. Las directrices dictadas por dichos organismos están encaminadas a establecer un conjunto de principios, derecho, obligaciones y procedimientos mínimos que deben ser respetados para la protección efectiva de este derecho, constituyen un positivo avance en la materia. No obstante, por carecer de fuerza jurídica vinculante para los países miembros de las respectivas organizaciones, salvo lo que disponen ellas mismas respecto de sus miembros, su cumplimiento queda supeditado a la voluntad de los Estados miembros.

Por otra parte, en el ámbito europeo, han surgido dos instrumentos internacionales que han sido claves en el proceso de desarrollo y consolidación del derecho fundamental a la protección de datos personales. Se trata, del Convenio nº 108 del Consejo de Europa, de 1981, para la protección de las personas con respecto al

[257] Al respecto, Isabel DAVARA FERNANDEZ, señala uno de los factores que complica llegar a un acuerdo internacional sobre protección de datos, sería que este es un derecho fundamental desconocido e infravalorado. Además, que «aún no se puede decir que se encuentre en igualdad de condiciones, en la práctica al menos, respecto de los demás derechos fundamentales». Cfr. *Hacia la estandarización de la protección de datos personales*, La Ley, Madrid, 2011, p. 467.

[258] Antonio TRONCOSO REIGADA, *La protección de Datos Personales. En Busca del equilibrio*, Tirant lo Blanch, Valencia, 2010, p. 244.

tratamiento automatizado de datos de carácter personal, su Protocolo Adicional de 2001 y de 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 cuanto a la validez de ambos instrumentos para servir de estándar internacional, ambos han corrido distinta suerte.

La Directiva 95/46/CE es una norma obligatoria y vinculante, pero sólo para los países miembros de la Unión Europea. No obstante, algunos autores plantean que la Directiva señalada se habría transformado de *facto* en un estándar internacional. Se llega a tal conclusión a partir del artículo 25 de la Directiva, que se refiere a la evaluación del «nivel adecuado» de protección que deben brindan terceros países para ser destinatarios de transferencias internacionales de datos personales desde la Unión Europea. Estos autores plantean que «si la propia Directiva establece una pléyade de parámetros para evaluar si un tercer país o una solución contractual cumple con "el nivel adecuado", en realidad lo que está planteando es una suerte de estándar». No obstante, agregan, «es un estándar limitado, porque se confiere a un país/organización/destinatario en concreto, y porque tiene que ser examinado y concedido en su caso tras un arduo proceso examinador y deliberativo, caso por caso». De cualquier forma, para ellos la Directiva europea, constituye un **"principio de estándar"**.[259] A nuestro juicio, imponer la Directiva europea como parámetro rector universal de lo que se debe considerar como un «nivel de protección adecuado», es excesivo. Por el contrario, creemos que es necesario avanzar hacia el establecimiento de un Convenio universal vinculante que haga uso, consagre y complemente los principios comunes de protección de datos y de respeto a la privacidad enunciados en los diferentes instrumentos existentes, extrayendo de ellos, en su conjunto, los principios, derechos, obligaciones y garantías mínimas a respetar.

Por su parte, el Convenio 108 del Consejo de Europa también es un instrumento de carácter regional europeo, pero con *vocación de universalidad*, ya que su artículo 23 permite la adhesión de Estados no miembros. Este Convenio ha sido el documento base para la discusión de una norma internacional para la protección de datos personales. De

[259] Por tados, véase Isabel DAVARA FERNÁNDEZ DE MARCO, *Hacia la estandarización de la protección de datos personales*, La Ley, Madrid, 2011, p. 471; y RAAB, C. D. & BENNETT, C. J., «Protecting Privacy Across Borders: European Policies and Prospects», *Public Administration*, volumen 72, marzo, 1994.

hecho, la Conferencia Internacional de Autoridades de Protección de Datos de 2009, donde se adoptó la Resolución sobre estándares internacionales en materia de protección de datos y privacidad, expresó su apoyo a los esfuerzos del Consejo de Europa para impulsar este derecho e invitó a los Estados, sean o no miembros de la organización, a ratificar el Convenio.[260]

No obstante, hay que reconocer que tanto la Directiva 95/46/CE como el Convenio 108, son documentos creados para el entorno europeo. Para avanzar en una normativa internacional de protección de datos, es indispensable una visión más amplia que acoja otras realidades y formas de analizar la materia, como ocurre en el ámbito geográfico americano y de Asia-Pacífico. Además, hay que tener en cuenta la desactualización de ambos instrumentos. El Convenio 108, al igual que la Directiva 95/46/CE, si bien están centrados en los principios y derechos y son tecnológicamente neutrales y, por tanto, suficientemente flexibles, nacen a comienzos de los años ochentas y mediado de los noventas del siglo pasado, respectivamente, por lo que no han podido contener una referencia más expresa a los nuevos tratamientos de datos personales derivados de la revolución de las TIC.[261]

4.2. Los Estándares internacionales sobre privacidad y protección de datos. Un primer paso hacia un Convenio universal

El primer paso para conseguir el objetivo de un Convenio universal sobre la materia, es la elaboración de unos «estándares internacionales sobre privacidad y protección de datos personales», que cuente con la mayor adhesión posible. No obstante, que desde hace largo tiempo existía la conciencia de la necesidad e importancia de un instrumento de estas características, no fue sino hasta pocos años atrás, que se da un impulso definitivo para la consecución de dicho fin.[262] Con la

[260] Cfr. Nota Explicativa —a la Resolución de Madrid—, sobre la Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal, acogida favorablemente por la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada el 5 de noviembre de 2009 en Madrid.

[261] En el mismo sentido, véase TRONCOSO REIGADA, Antonio, *La protección de Datos Personales. En Busca del equilibrio,* Tirant lo Blanch, Valencia, 2010, p. 249.

[262] Antonio TRONCOSO REIGADA, señala al respecto que «posiblemente existía un cierto escepticismo —o pesimismo— acerca de las posibilidades reales de alcanzar tan ambicioso objetivo, que olvidaba la importancia de ir dando pasos concretos —aunque fueran pequeños— en esa dirección». Cfr. *La protección de Datos Personales. En Busca del equilibrio,* Tirant lo Blanch, Valencia, 2010, p. 245.

aprobación por unanimidad, en la 30ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada en Estrasburgo en 2008, es cuando empieza a tomar forma la Resolución para elaborar una Propuesta Conjunta para el establecimiento de estándares internacionales sobre privacidad y protección de datos. La Agencia Española de Protección de Datos junto con el Comisionado Federal de Protección de Datos de Suiza, fueron los principales promotores de dicha iniciativa.

La Conferencia creó un grupo de trabajo, con el objetivo de trabajar en las diferentes partes de la propuesta.[263] El proceso de elaboración de esta propuesta conjunta contó con una amplia participación, en los grupos de trabajo, foros o audiencias que se realizaron, de entidades y organizaciones tanto públicas como privadas, lo que le permitió lograr un amplio consenso institucional y social. También, se prestó particular atención a los trabajos puestos en marcha por la Organización Internacional de Estandarización (normas ISO)[264] y por la Comisión de Derecho Internacional de Naciones Unidas.

Para la elaboración de la propuesta se consultaron los diferentes textos legales, directrices y recomendaciones de alcance internacional que han recibido un amplio consenso en sus respectivos ámbitos geográficos, económicos o legales de aplicación, como son los instrumentos de la OCDE, APEC, ONU y de la Red Iberoamericana de Protección de Datos. De esta forma, la propuesta se ha elaborado asumiendo que todos estos principios y enfoques comunes aportan elementos de valor en la defensa y la

[263] Los criterios rectores para dicho trabajo fueron: recurrir a los principios y derechos relacionados con la protección de datos personales en los diversos entornos geográficos del mundo, con atención particular a textos, legales o no, que hayan logrado un amplio consenso en sus respectivos foros regionales o internacionales; Elaborar un conjunto de principios y derechos que, reflejando y completando los textos existentes, permitan alcanzar el mayor grado de aceptación internacional asegurando un alto nivel de protección; evaluar los sectores en los que resultan aplicables dichos principios y derechos, incorporando alternativas dirigidas a armonizar su ámbito de aplicación; definir, atendiendo a los diversos sistemas jurídicos, los criterios básicos que garanticen su aplicación efectiva; valorar la función que puede desempeñar la autorregulación; formular las garantías exigibles para permitir de forma ágil y flexible las transferencias internacionales de datos. Cfr. la 30ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad Estrasburgo, del 15 al 17 de octubre de 2008, *http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Cooperation/Conference_int/08-1017_Strasbourg_social_network_ES.pdf* [fecha consulta: 27.11.2011]

[264] Sobre el Este tipo de normas y su fomento por parte de las Autoridades de Protección de Datos, véase la 29ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada en Montreal, Canadá, del 26 al 28 de septiembre de 2007, donde se aprobó la Resolución relativa a la elaboración de normas internacionales, *http://www.privacyconference2007.gc.ca/Global%20Standards%20Resolution%20-%20Spanish.pdf* [fecha consulta: 20.10.2011]

mejora de la privacidad e información personal, con el objetivo de ampliarlos mediante soluciones y disposiciones específicas que podrían aplicarse independientemente de las diferencias que puedan existir entre los diferentes modelos existentes de protección de datos y privacidad.

Finalmente, la Resolución de Estándares Internacionales fue aprobada por la 31ª Conferencia Internacional sobre Privacidad y Protección de Datos celebrada en Madrid en 2009 —más conocida como Resolución de Madrid—.[265] Ésta supone un equilibrio entre las diferentes visiones sobre las protección de datos personales existentes a nivel internacional y que plasman en las distintas legislaciones. Es por tanto, un documento nacido del diálogo y de la búsqueda del consenso que trata de integrar sensibilidades de los distintos continentes, recogiendo los principios que son comunes a todos los modelos.[266] Como señaló el Presidente de la Agencia Española de Protección de Datos en la presentación de la Resolución, «su carácter consensuado aporta dos valores añadidos esencialmente novedosos: de un lado, enfatiza la vocación universal de los principios y garantías; del otro, reafirma la factibilidad de avanzar hacia un documento internacionalmente vinculante, que contribuya a una mayor protección de los derechos y libertades individuales en un mundo globalizado y, por ello, caracterizado por las transferencias internacionales de información».[267]

El objeto de la Resolución de Madrid, es «definir un conjunto de principios y derechos que garanticen la efectiva y uniforme protección de la privacidad a nivel internacional, en relación con el tratamiento de datos de carácter personal» (art. 1). Para ello, la propuesta se articula con unos principios de protección de datos básicos, unos

[265] Cfr. «La Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal», acogida favorablemente por la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada el 5 de noviembre de 2009 en Madrid. Para una mayor información sobre el desarrollo de los trabajos preparatorios de este documento, véase web de la Agencia Española de Protección de Datos, *www.agpd.es*

[266] Podemos decir, por tanto, que se cumplió con el mandato impuesto en la Resolución de Estrasburgo, que imponía como criterio rector que «el proceso de elaboración de ésta Propuesta Conjunta debe desarrollarse fomentando una amplia participación, en los grupos de trabajo, foros o audiencias que se realicen, de entidades y organizaciones tanto públicas como privadas, con el fin de lograr el más amplio consenso institucional y social». Para Antonio Troncoso, «así ha sido ya que en los distintos grupos de trabajo han participado no sólo representantes de las autoridades sino también de la sociedad civil, la industria y la Universidad». Cfr. TRONCOSO REIGADA, Antonio, *La protección de Datos Personales. En Busca del equilibrio*, Tirant lo Blanch, Valencia, 2010, p. 246.

[267] Cfr. Artemi RALLO, "Presentación" a *Estándares Internacionales sobre Protección de Datos Personales y Privacidad*, AEPD. *http://www.privacyconference2009.org/home/index-ides-idweb.html*

derechos de protección de datos de los interesados y unas obligaciones de cumplimiento y supervisión. En el apartado VI se desarrollan los puntos sobre los cuales se logró alcanzar un consenso entre todas las partes que participaron de la misma. Así, en la primera parte, se otorgan algunas definiciones básicas y determinar su ámbito de aplicación. La segunda parte se encarga de consagrar los principios básicos sobre el tratamiento de datos personal, estos son, los principios de lealtad y legalidad, de finalidad, de proporcionalidad, de calidad, de transparencia y de responsabilidad. La tercera parte se dedica a regular los supuestos que legitiman el tratamiento de datos personales, señala los requisitos para que un dato de carácter personal sea considerado sensible e indica las condiciones para que el responsable pueda encargar el tratamiento de datos a uno a varios prestadores de dicho servicio (encargados del tratamiento). Además, contempla los requisitos y condiciones para realizar una transferencia internacional de datos personales. La cuarta parte se destina a regular los derechos de la persona interesada o afectada, como los derechos de acceso, rectificación, cancelación y oposición. Además, establece la forma y condiciones para garantizar el ejercicio de dichos derechos. La quinta parte se destina a regular la seguridad. En la última parte, se entregan algunas disposiciones sobre el cumplimiento y supervisión de la misma.

No obstante su importancia, hay que tener en cuenta que estos instrumentos carecen de fuerza normativa, es decir, no son vinculantes para los Estados.[268] Es por ello que se debe avanzar en la concreción de un acuerdo internacional específico sobre el derecho a la protección de datos y la privacidad, que sea aceptado, ratificado e implantado en la mayor cantidad de países posibles, a objeto de cautelar de forma efectiva este derecho en el nuevo entorno mundial. Para contar con un instrumento normativo internacional «es necesario que su aprobación siga las reglas del Derecho Internacional Público, lo que requiere la intervención de representantes de los Estados y un largo proceso de maduración».[269] La propia Resolución de Madrid «expresa la

[268] Como lo destaca TRONCOSO, «la Conferencia Internacional de Protección de Datos y la Conferencia de Primavera —de autoridades europeas—no están constituidas en virtud de Tratados o Convenio Internacionales y, por tanto, no se trata de la participación en ninguna organización internacional regida por el Derecho Internacional general. Estas Conferencias son un foro de debate teórico sobre cuestiones de actualidad que afectan a la protección de datos personales y de intercambio de experiencias de las distintas Autoridades que tienen que aplicar en el día a día el derecho fundamental». En definitiva, las Declaraciones, Resoluciones y Acuerdos que tome la Conferencia carecen de valor jurídico, en el sentido de ser vinculante para los Estados. Cfr. TRONCOSO REIGADA, Antonio, *La protección de Datos Personales. En Busca del equilibrio,* Tirant lo Blanch, Valencia, 2010, p. 247.

[269] Cfr. Antonio TRONCOSO REIGADA, *La protección de Datos Personales.* op. cit., p. 247.

convicción de la Conferencia de que el reconocimiento de estos derechos pasa por la adopción de un instrumento legislativo universal y vinculante, que haga uso, consagre y complemente los principios comunes de protección de datos y de respeto a la privacidad enunciado en los diferentes instrumentos existentes y que refuerce la cooperación internacional entre autoridades de protección de datos».[270]

Para concluir, podemos señalar, que la necesidad de contar con un convenio jurídico universal y vinculante, tecnológicamente neutral y certificable en materia de protección de datos personales y privacidad es evidente y urgente. En este sentido, la Resolución de Madrid que consagra unos estándares internacionales sobre privacidad y protección de datos, es vista como un medio para alcanzar dicho fin.[271]

[270] Cfr. Nota explicativa de la Resolución de Madrid.
[271] En el mismo sentido, véase el apartado 4 de la Resolución.

SEGUNDA PARTE

MARCO NORMATIVO DE LA PROTECCIÓN DE DATOS CON FINES DE PREVENCIÓN Y REPRESIÓN PENAL EN LA COOPERACIÓN POLICIAL EUROPEA

CAPITULO CUARTO

NORMATIVA DEL CONSEJO DE EUROPA Y SU IMPORTANCIA PARA LA MATERIA EN ESTUDIO

SUMARIO: INTRODUCCIÓN; 1. CONVENIO EUROPEO DE DERECHO HUMANOS (Artículo 8º); 2. CONVENIO 108 DEL CONSEJO DE EUROPA, DE 28 DE ENERO DE 1981, COMO REGLA MÍNIMA APLICABLE; 3. RECOMENDACIÓN N º R (87) 15, DEL CONSEJO DE EUROPA, QUE REGULA LA UTILIZACIÓN DE DATOS PERSONALES EN EL SECTOR DE LA POLICÍA, COMO BASE JURÍDICA DE FACTO EN LA MATERIA.

INTRODUCCIÓN

Para hablar del marco normativo actualmente aplicable a la protección de datos personales en el ámbito de la prevención y represión penal en Europa, necesariamente tenemos que recurrir, por una parte, al proceso evolutivo que ha sufrido este derecho fundamental, y por otra, hacer mención de las diversas fuentes de las cuales proviene su regulación. Sólo de esta forma, se comprende a cabalidad la superposición de normas, tanto supranacionales provenientes de los convenios del Consejo de Europa como de las normas emanadas de las diversas fases del proceso de consolidación de la Unión. Es por ello que este trabajo recoge los instrumentos legislativos vigentes en materia de protección de datos proveniente tanto del Consejo de Europa como de la Unión Europea.

Esta fuente bicéfala de generación de normas, ha permitido que Europa se convierta en uno de los ámbitos político geográfico donde el derecho fundamental a la protección de datos ha tenido mayor desarrollo. Desde la labor pionera desarrollada por el Consejo de Europa a partir de la década de los sesentas, hasta la consagración definitiva de la protección de datos personales como derecho fundamental autónomo en el artículo 8º de la Carta Europea de Derechos Fundamentales, a principios del presente siglo, se puede ver la evolución y adaptación de este derecho en la jurisprudencia,

doctrina y legislación Europea y de los Estados miembros. Lo anterior, no lleva a afirmar que Europa es la zona jurídica donde se brinda a los ciudadanos los más altos estándares de protección en la materia.

El estudio de esta segunda parte, referido al marco jurídico de la protección de datos en Europa, lo hemos dividido en tres capítulos. El capítulo cuarto, lo destinamos al análisis de las normas provenientes del Consejo de Europa. Los capítulos quinto y sexto, los dedicamos al estudio de las normas provenientes de la Unión Europea, distinguiendo a su vez, entre normas generales sobre protección de datos y aquellas dictadas específicamente para el ámbito de la prevención y sanción penal o que tienen incidencia en ella.

El Consejo de Europa es una de las organizaciones política intergubernamental más antigua de los Estados europeos.[272] De acuerdo con sus Estatutos el Consejo de Europa tiene por finalidad proteger los Derechos Humanos y la primacía del derecho en todos los Estados Miembros; consolidar la estabilidad democrática de Europa, respaldando la reforma constitucional, política y jurídica en los planos nacional, regional y local; hallar soluciones a problemas sociales, los problemas de la discriminación hacia las minorías, de la xenofobia, de la intolerancia, de la violencia contra la infancia; promover y desarrollar la identidad cultural europea; la cohesión social y los derechos sociales, prestando particular atención a la educación.[273] Con el transcurso de los años, se han añadido otras finalidades como la bioética, la clonación, el terrorismo, el tráfico de seres humanos, el crimen organizado, la corrupción y la ciber-criminalidad.

En el ámbito específico de la protección de datos personales, la labor desarrollada por el Consejo de Europa puede ser calificada de fundadora. Ya a fines de la década de

[272] Se estableció con posterioridad a la II Guerra Mundial (1949) con sede permanente en Estrasburgo, Francia. Actualmente lo integran 47 Estados, que van desde Finlandia hasta Turquía y desde Portugal a Rusia y su Asamblea Parlamentaria representa a más de 800 millones de personas. Formado inicialmente sólo por 10 Estados de Europa Occidental, el Consejo de Europa estaba destinado a abarcar todos los países del continente, pero la Guerra Fría retrasó su ampliación. Es por ello que sólo a partir de 1989 el Consejo de Europa se ha convertido en una organización verdaderamente paneuropea. Además están presentes en ella, en calidad de observadores, la Santa Sede, Estados Unidos, Canadá, Japón y México. Para una revisión de la historia, actividades y logros del Consejo de Europa, véase Aline Royer, The Council of Europe, disponible en http://book.coe.int/

[273] Cfr. Estatuto del Consejo de Europa, hecho en Londres el 5 de mayo de 1949. El Instrumento de Adhesión de España al Estatuto del Consejo de Europa, se publicó en el BOE núm. 51/1978, de 1.3.1978.

los años sesenta y principio de los setenta, existía conciencia en este organismo de las potenciales amenazas que representaba el procesamiento de datos personales a través de medios informáticos para la vida privada de los sujetos. Esta preocupación por parte del Consejo de Europa sobre la regulación de los datos de carácter personal, junto con dar protección a la privacidad de los individuos, también obedecía a la necesidad de dar claridad y certeza jurídica respecto del tráfico internacional de datos personales. Se buscaba ya desde entonces, facilitar el intercambio de datos y las relaciones institucionales y comerciales entre los distintos países, evitando los paraísos de datos.[274]

Si se analizan los diversos instrumentos normativos del Consejo de Europa sobre protección de datos de carácter personal, se puede observar una estrecha relación de contenidos y fines entre éstos y las Directrices de la OCDE, ONU y con la normativa de la Comunidad Europea. En todos ellos encontraremos la constante de establecer los principios esenciales que rigen el tratamiento de datos personales, determinar las obligaciones y derechos de los involucrados en el tratamiento, como también, la necesidad de establecer ciertas garantías institucionales para el efectivo cumplimiento de este derecho.[275]

Dos son los instrumentos internacionales del Consejo de Europa que han tenido mayor impacto en el desarrollo del derecho a la protección de datos, el Convenio Europeo de Derechos Humanos, también conocido como el Convenio de Roma de 1950 (en adelante, CEDH)[276] y el Convenio núm. 108 del Consejo de Europa (en adelante, Convenio 108).[277] El primero consagra por primera vez a nivel europeo la tutela de la vida privada, y el segundo define desde una perspectiva normativa el contexto de

[274] Antonio TRONCOSO REIGADA, *La protección de datos personales: en busca del equilibrio* (Tirant lo Blanch, 2010), p. 56.

[275] Estos instrumentos generados por organizaciones intergubernamentales —Resoluciones y Recomendaciones del Comité de Ministros del Consejo de Europa; Directrices del Consejo de la Organización de Cooperación y Desarrollo Económico (OCDE); y Resoluciones de la Asamblea General de las Naciones Unidas (ONU)— en los que tomaron cuerpo un conjunto de principios, aceptados por la mayoría de Estados, en materia de tratamiento automatizado de datos de carácter personal. En el caso de España, la integración en la Comunidad Europea impuso al legislador nacional español el deber de tener en cuenta las normas comunitarias de Derecho derivado existentes en la materia. Al respecto véase Olga ESTADELLA YUSTE, *La protección de la intimidad frente a la transmisión internacional de datos personales* (Madrid: Tecnos, 1995), p. 59-75; Mónica ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa* (Valencia: Tirant lo Blanch, 2006), p. 151.

[276] España firmó el Convenio de Roma el 24 de noviembre de 1977 y lo ratificó el 26 de septiembre de 1979. BOE núm. 243, de 10 de octubre de 1979.

[277] Convenio del Consejo de Europa de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Ratificado por España el 27 de enero de 1984. BOE de 15 de noviembre de 1985.

protección de la privacidad en relación con las TIC.[278] También en el ámbito específico del tratamiento de datos personales por parte de la policía, el Consejo de Europa ha hecho su aporte, al proponer a los Estados Miembros la primera Recomendación que orienta la labor policial en el tratamiento de datos personales.[279] Como analizaremos al final de este apartado, dicha recomendación ha sido considerada por todos los instrumentos normativos elaborados por la Unión Europa referido al tema específico del tratamiento de datos con fines de represión y prevención penal. Incluso la nueva Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales con fines de prevención y represión penal, hace mención en su exposición de motivos a esta Resolución del Consejo de Europa.[280]

1. CONVENIO EUROPEO DE DERECHO HUMANOS (artículo 8º)

La importancia que le brinda a los derechos fundamentales el Consejo de Europa, queda de manifiesto en el hecho que el primer Convenio que celebra, es el Convenio Europeo de Derechos Humanos.[281] Este tratado internacional de carácter regional, contiene un catálogo de derechos y libertades fundamentales que los Estados firmantes se comprometen a respetar y garantizar.[282] La relevancia que ha adquirido

[278] Simultáneamente a estos Acuerdos Internacionales del Consejo de Europa aparecieron otros instrumentos generados por diversas organizaciones intergubernamentales —Resoluciones y Recomendaciones del Comité de Ministros del Consejo de Europa, Directrices del Consejo de la Organización de Cooperación y Desarrollo Económico (OCDE), y Resoluciones de la Asamblea General de las Naciones Unidas (ONU)— donde se establecen un conjunto de principios, aceptados por la mayoría de Estados, en materia de tratamiento automatizado de datos de carácter personal. Al respecto véase Ricard MARTÍNEZ MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa*, p. 157; ESTADELLA YUSTE, *La protección de la intimidad frente a la transmisión internacional de datos personales*, p. 59–75.

[279] Recomendación n º r (87) 15, del Consejo de Europa, que regula la utilización de datos personales en el sector de la policía, de 17 de septiembre 1987. Al respecto véase *infra* aparado 3 de este capítulo.

[280] Cfr. COM/2012/010 final-2012/0010(COD). Disponible en la página web de la Unión Europea: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0010:ES:HTML*. [consulta: 05.04.2013].

[281] Firmado el 4 de noviembre de 1950, entró en vigor el 3 de septiembre de 1953, tras el depósito de los diez instrumentos de ratificación, que exigía el artículo 66.2 del Convenio. La lista completa de los Tratados suscritos por el Consejo de Europa se encuentra disponible en *http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=8&CL=ENG* [consulta: 9.7.2013]

[282] Sobre el Convenio Europeo de Derechos Humanos existe una abundante bibliografía, entre otros, véase Mónica ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, pp. 43-150; Joaquín BRAGE CAMEZANO, «Aproximación a una teoría general de los derechos fundamentales en el Convenio Europeo de Derechos Humanos», *Revista Española de Derecho Constitucional* n.º 74 (2005): pp. 111-138; Juan Antonio CARRILLO SALCEDO, *El Convenio Europeo de Derechos Humanos*, 2003; Ángel Gregorio CHUECA SANCHO, «Por una Europa de los derechos

para el Consejo de Europa el CEDH queda en evidencia en el hecho que actualmente la adhesión al Consejo de Europa por parte de nuevos Estados está subordinada a la firma y ratificación del CEDH.[283]

El CEDH se inspira en otros catálogos internacionales de derechos, como son la Declaración Universal de Derechos Humanos (en adelante, DUDH)[284] y el Pacto Internacional de Derechos Civiles y Políticos (en adelante PIDCP).[285] Sin embargo, existen importantes diferencias entre aquél y éstos. En primer lugar, el CEDH es un tratado internacional y, por tanto, está dotado de la obligatoriedad, en cambio la DUDH carece de ella. Y, en segundo lugar, el CEDH establece un sistema de garantías judiciales internacionales para controlar el respeto de los derechos reconocidos en el mismo y que la DUDH tampoco establece.[286] De esta forma «ante la escasa virtualidad de otros textos Internacionales el Convenio de 1950 ha resultado particularmente eficaz en el ámbito de la protección de los Derechos Humanos en aquellos Estados que han aceptado ser vinculados por sus mandatos».[287]

---

humanos: la adhesión de la Unión Europea al Convenio Europeo de Derechos Humanos», en *Unión Europea y Derechos fundamentales en perspectiva constitucional*, ed. N. FERNÁNDEZ SOLA (Madrid: Dykinson, 2004), pp. 37-58; Carmen MORTE GÓMEZ y Guillem CANO PALOMARES, «La interpretación evolutiva y dinámica del Convenio Europeo de Derechos Humanos en la jurisprudencia reciente del Tribunal de Estrasburgo», *Revista general de derecho constitucional*, 10 (2010): pp. 14 y ss.

[283] Aunque esta práctica comenzó con las adhesiones de Portugal, España y Finlandia, no quedó formalizada sino hasta la Declaración de Viena de 9 de octubre de 1993. Entre las causas probables de este cambio, Mónica Arenas plantea que «debido a los profundos cambios surgidos en Europa, fundamentalmente, como consecuencia del desmembramiento del bloque soviético en 1990, la adhesión al Consejo de Europa está subordinada, ahora, a una condición política: firma y ratificación del CEDH. Formar parte del CEDH se convierte en una exigencia del Comité de Ministros para la adhesión a la organización». Cfr. Mónica ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, pp. 43–44.

[284] Declaración Universal de los Derechos Humanos, aprobada por la Asamblea General de las Naciones Unidas, el 10 de diciembre de 1948. Disponible en: http://www.un.org/es/documents/udhr/ [consulta: 9.7.2013]. Sobre la Declaración Universal de Derechos Humanos, véase Jaume SAURA ESTAPÀ, «Comentario al artículo 12 de la Declaración Universal de los Derechos Humanos», en *La Declaración Universal de los Derechos Humanos*, ed. X. PONS RAFOLS (Barcelona: Asociación para las Naciones Unidas en España-Icaria, 1998), pp. 226-236; Jaime ORAÁ y Felipe GÓMEZ ISA, *La Declaración Universal de los Derechos Humanos: Un Breve comentario en su 50 aniversario*, 2° ed. (Bilbao: Universidad de Deusto, 2002); Antonio CARRILLO SALCEDO, *Dignidad frente a barbarie: la Declaración Universal de Derechos Humanos cincuenta años después* (Madrid: Trotta, 1999).

[285] Pacto Internacional de Derechos Civiles y Políticos. Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General de la Naciones Unidas, en su resolución 2200 A (XXI), de 16 de diciembre de 1966. Entro en vigor el 23 de marzo de 1976. Disponible en http://www2.ohchr.org/spanish/law/ccpr.htm [consulta: 9.7.2013]

[286] El sistema de protección del CEDH se judicializa con la la entrada en vigor del Protocolo núm. 11 en 1998.

[287] Ricard MARTÍNEZ MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa*, 157.Martínez Martínez, *Una aproximación crítica a la autodeterminación informativa*, p. 157.

El Convenio de Roma, de 1950, para la Protección de los Derechos Humanos y de las Libertades Fundamentales tiene la virtud de ser el primer texto europeo que consagra la tutela de la vida privada, afirmando en su artículo 8: «1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencias de la autoridad pública en el ejercicio de este derecho sino en tanto esta injerencia esté prevista por ley y constituya una medida que, en una sociedad democrática sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».[288] Como se puede apreciar, el precepto se limita a enunciar un conjunto de derechos sin mayor concreción. Es por ello que el contenido efectivo de este precepto ha sido precisado a través de la jurisprudencia del Tribunal Europeo de Derechos Humanos (en adelante, TEDH).[289]

El derecho al respeto a la vida privada y familiar consagrado en el artículo 8 del CEDH, corresponde, a nuestro juicio, a los llamados derechos personalísimos o de la personalidad, esto es, los que se encuentran ligados a la existencia misma del individuo. Su finalidad es permitir a las personas un ámbito propio y reservado, necesario para el desarrollo de la personalidad.[290] Al permitir a las personas poseer un ámbito propio y

[288] El artículo 8 del CEDH, sigue de cerca los artículos 12 de la Declaración Universal de Derechos Humanos y 17 del Pacto Internacional de Derechos Civiles y Políticos. El artículo 12 del CEDH establece que «nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques». Por su parte, el artículo 17 del PIDCP, señala que «1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques». Algunos autores plantean un matiz de diferenciación del artículo 8 del CEDH, al señalar que dicho artículo no reconoce un *derecho* a la vida privada, sino el *derecho al respeto* a la vida privada. Cfr. Mónica ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, p. 55.

[289] Al respecto, véase Xabier ARZOZ SANTIESTEBAN, «Artículo 8: derecho al respeto de la vida privada y familiar», en *Convenio Europeo de Derechos Humanos. Comentario sistemático*, ed. Iñaki LASAGABASTER HERRARTE (Navarra: Thomson-Reuters Civitas, 2009); RUIZ MIGUEL, Carlos, *El Derecho a la Protección de la Vida Privada en la Jurisprudencia del Tribunal Europeo de Derechos Humanos* (Civitas, 1994); Mónica ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa* (Valencia: Tirant lo Blanch, 2006), pp. 54-86; Carmen MORTE GÓMEZ y Guillem CANO PALOMARES, «La interpretación evolutiva y dinámica del Convenio Europeo de Derechos Humanos en la jurisprudencia reciente del Tribunal de Estrasburgo», *Revista general de derecho constitucional* 10 (2010): pp. 14 y ss.

[290] En el mismo sentido Mónica Arenas, señala que «todos los bienes jurídicos protegidos por el artículo 8 del CEDH sirven al objetivo de garantizar esa cierta esfera autónoma de actuación y desarrollo personal». Cfr. ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, 55.

reservado, se cautela el libre desarrollo de su personalidad, necesario para mantener una calidad de vida mínima en sociedad.

Desde esta óptica, si se analizan los bienes jurídicos protegidos por el artículo 8 del CEDH (vida privada, vida familiar, el domicilio y la correspondencia), comprobamos que todos ellos sirven al objetivo de garantizar esa cierta esfera autónoma de actuación y desarrollo personal.[291] En esta línea, el TEDH ha señalado que la garantía que ofrece el artículo 8 del CEDH está principalmente destinada a garantizar el desarrollo, sin injerencias externas, de la personalidad de cada individuo en las relaciones con sus semejantes, es decir, a cada individuo se le garantiza un espacio en el cual pueda llevar a cabo libremente el desarrollo y la realización de su personalidad.[292]

La protección de datos personales no se encuentra regulada de forma explícita como un derecho fundamental autónomo en el CEDH.[293] Ello es lógico toda vez que el derecho fundamental a la protección de datos es un derecho nuevo, que ha tenido un mayor impulso y desarrollo a partir del surgimiento de la informática como medio de procesar información de carácter personal, lo que se produjo con posterioridad a la aprobación del Convenio de Roma en 1950. Su inclusión ha sido fruto de una interpretación amplia o extensiva del término «vida privada» que ha realizado el Tribunal Europeo de Derechos Humanos respecto del artículo 8º del CEDH.[294] De esta forma, el TEDH ha incluido dentro del ámbito o campo de protección del artículo 8 del CEDH la recogida, almacenamiento o difusión de datos personales de cualquier tipo.[295] Para el TEDH los datos personales forman parte de la «esfera privada» y, en

[291] Ídem.

[292] Cfr. SSTEDH caso *Dudgeon* , de 22 de octubre de 1981; caso *Botta*, de 24 de febrero de 1998; caso N. F. vs. Italia, de 2 de agosto de 2001; caso *Peck*, 28 de enero de 2003; y los casos *I. vs. Reino Unido* y *Goodwin*, ambas de 11 de julio de 2002.

[293] Para un estudio detallado sobre los bienes jurídicos protegidos por el artículo 8º del CEDH y la forma como el Tribunal Europeo de Derechos Humanos ha incorporado la protección de datos personales dentro del ámbito protegido por el derecho al respeto a la vida privada y familiar, véase Mónica ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, pp. 54–146; ARZOZ SANTIESTEBAN, "Artículo 8: derecho al respeto de la vida privada y familiar"; Carlos RUÍZ MIGUEL, *El Derecho a la Protección de la Vida Privada en la Jurisprudencia Del Tribunal Europeo de Derechos Humanos* (Civitas, 1994).

[294] Cfr. SSTEDH: *Leander*, de 26 de marzo de 1987; *Gaskin*, de 7 de julio de 1989; *Guerra* y otros, de 19 de febrero de 1998; *Fressoz y Roire*, de 21 de enero de 1999; *Amann*, de 16 de febrero de 2000; *Rotaru*, de 4 de mayo de 2000; y *Odeivre*, de 13 de febrero de 2003.

[295] Cfr. SSTEDH caso *Fressoz y Roire*, de 21 de enero de 1999; caso *Rotaru* , de 4 de mayo de 2000; caso *Amann*, de febrero de 2000.

consecuencia, del ámbito protegido por el derecho a la vida privada reconocido en el artículo 8 del CEDH. Esta postura del TEDH, de reconocer y garantizar el derecho a la protección de datos personales, ha contribuido a la creación de un estándar mínimo sobre la materia, al buscar una postura unánime entre los diferentes sistemas jurídicos.[296]

El proceso de reconocimiento y garantía del derecho a la protección de datos dentro del artículo 8 del CEDH fue gradual, y en él fueron fundamentales las Resoluciones y Recomendaciones que dictó el Consejo en diversas áreas en la década de los 70' y 80', y se vio aún más reforzada con la elaboración y aprobación del Convenio 108 sobre protección de datos personales del año 1981, que pasamos a revisar a continuación.

2. CONVENIO 108 DEL CONSEJO DE EUROPA, DE 28 DE ENERO DE 1981, COMO REGLA MÍNIMA APLICABLE

El nacimiento, desarrollo y uso extensivo de la informática en Europa, hizo necesario conciliar, por una parte, la necesidad de facilitar el libre tránsito de la información entre personas e instituciones públicas y privadas, y por otra, la de cautelar los derechos de las personas frente a las amenazas del procesamiento de datos. Con este doble fin surge el Convenio nº 108, de 28 de enero de 1981, del Consejo de Europa, para la protección de las personas respecto al tratamiento automatizado de los datos de carácter personal, que pasa a ser el primer texto jurídico vinculante con vocación universal en el ámbito de la protección de datos.[297] De esta forma, se intenta satisfacer la necesidad social de profundizar la protección de los derechos de los individuos, en especial en lo relativo a la vida privada, consagrada por el artículo 8.1 del CEDH en relación con el uso de la informática.

[296] Al respecto Mónica Arenas, señala que «la mayoría de los Estados firmantes del CEDH no reconocen expresamente en sus Constituciones un derecho fundamental a la protección de datos, sino que ha sido sus Tribunal constitucionales los que han ido interpretando que la protección de datos personales quedaba incluida, bien dentro del ámbito protegido por el derecho a la vida privada, o bien dentro del ámbito protegido por otro derecho fundamental». Por este motivo, concluye, «el TEDH ha jugado un papel determinante en el reconocimiento y garantía del derecho a la protección de datos personales creando un estándar mínimo sobre la materia». Cfr. ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, pp. 79.

[297] Hasta ahora, lo han firmado y ratificado 46 de los 47 Estados Miembros del Consejo. El último Estado en ratificarlo, durante el 2013 fue Uruguay. Cfr. *http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=09/07/2013&CL=ENG*

Este instrumento ha sido modificado y complementado en dos oportunidades. Se modificó por primera vez el 15 de junio de 1999[298], con el fin de permitir a la Comunidad Europea acceder al mismo; y el 8 de noviembre de 2001[299]; se complementó por medio de un Protocolo Adicional por cual se exigía la creación de autoridades de control independientes nacionales y se establecían las condiciones para la transferencia de datos personales a otros países u organizaciones que no fueran parte del mismo.[300]

La elaboración del Convenio 108 estuvo precedido por dos Resoluciones del Consejo de Ministros, la R (73) 22 y la R (74) 29, referidas a la protección de datos en los sectores privado y público respectivamente, que adelantaban algunos de los principios básicos que después inspirarían la redacción del Convenio de 1981.[301] Estas Resoluciones constituyen los primeros intentos de aproximación de las legislaciones de los Estados Miembros.[302]

---

[298] Modificaciones (enmiendas) al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, aprobado por el Comité de Ministros del Consejo de Europa, en Estrasburgo, el 15 de junio de 1999. Cabe recordar que el Tratado de Lisboa modificó el Tratado de la Unión Europea y al Tratado constitutivo de la Comunidad Europea a partir del 1 de diciembre de 2009, por tanto, a partir de esa fecha, cualquier referencia a las Comunidades Europeas se entenderá como la Unión Europea. Disponible en *http://conventions.coe.int/Treaty/EN/Treaties/Html/108-1.htm* [consulta: 09.07.2013]

[299] Protocolo Adicional a la Convención para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, relativo a las autoridades de control y los flujos transfronterizos de datos. Consejo de Europa, STE núm. 181, de 8 de noviembre de 2001. En vigor a partir del 01 de julio de 2004. Este instrumento no ha sido firmado ni ratificado por España. Disponible en *http://conventions.coe.int/Treaty/EN/treaties/html/181.htm*

[300] El propósito principal del Protocolo Adicional es reforzar la puesta en marcha y la aplicación efectiva de los principios contenidos en el Convenio 108. Esta necesidad de reforzamiento de dos aspecto esenciales en materia de protección de datos -autoridades de control y transferencia internacional de datos- se debe al extraordinario crecimiento experimentado de los flujos transfronterizos de los datos de carácter personal llevados a cabo desde un Estado parte en el Convenio hacia un tercer Estado u organización internacional que no lo sea, laguna que venía advirtiendo la doctrina al referirse a la formulación del artículo 12 del Convenio 108. Al respecto véase la Memoria Explicativa del Protocolo Adicional. Para un estudio detallado de este instrumento jurídico, véase Juan Antonio PAVÓN PÉREZ, «La protección de datos personales en el Consejo de Europa: el Protocolo Adicional al Convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales», *Anuario de la Facultad de Derecho (Universidad de Extremadura),* 2001-2002, pp. 235-252.

[301] Cfr. Resolución (73) 22 relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado, acordada por el Comité de Ministros el 26 de septiembre de 1973; y Resolución (74) 29 relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector público, adoptada por el Comité de Ministros el 20 de septiembre de 1974.

[302] Cabe recordar que previo a estas primeras Resoluciones específicas de la Asamblea del Consejo, se dictó en 1968 una que versaba sobre «los derechos humanos y los nuevos logros científicos y técnicos». http://conventions.coe.int

La importancia de estas Resoluciones radica en que consagra por primera vez principios esenciales sobre la materia que aún hoy se encuentran actualmente vigentes, como el de calidad de los datos, información sobre la finalidad, seguridad de los datos, derecho de acceso y cancelación, entre otros. Además, estas resoluciones, aun cuando carecen de fuerza jurídica vinculante, tienen el mérito de constituir los primeros textos a nivel internacional que contienen directrices dirigidas a los Estados, lo que influyó decisivamente en la legislación de esa época y permitió inicialmente la armonización paulatina y flexible de los textos legales europeos sobre protección de datos.[303]

El Comité de Ministros del Consejo de Europa, consciente de la necesidad de tener un texto jurídico vinculante para todos los Estados y con un carácter más amplio, adopta la Resolución (76) 3 de 18 de febrero de 1976, por la cual se constituye un Comité de Expertos en protección de datos. Éste Comité planteó dos opciones, o bien realizar un Protocolo Adicional, que complementara el artículo 8 del Convenio Europeo de Derechos Humanos, o bien, realizar un nuevo Convenio específico para la protección de datos personales que desarrollara el derecho al respeto a la vida privada consagrado en el art. 8 CEDH. Al final predominó esta segunda opción, básicamente con la finalidad de permitir la adhesión al Convenio de Estados miembros de la OCDE no Europeos (Canadá, Estados Unidos y Japón) por el mecanismo de la "invitación" del Comité de Ministros de Consejo de Europa, mediante el procedimiento consignado en el artículo 23.1 del Convenio nº 108.[304] Esto explica por qué la rúbrica formal del Convenio intencionadamente no incluye el adjetivo «europeo».[305]

La elaboración del Convenio estuvo a cargo de un Comisión de expertos gubernamentales del Comité Europeo de Cooperación Jurídica. También participaron en la preparación del mismo los cuatro miembros no europeos de la organización (Australia, Canadá, Japón y Estados Unidos), observadores de la OCDE y

[303] En el mismo sentido, véase Ricard MARTÍNEZ MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa*, p. 161.

[304] Artículo 23. *Adhesión de Estados no miembros.* 1. Después de la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa podrá invitar a cualquier Estado no miembro del Consejo de Europa a que se adhiera al presente Convenio mediante un acuerdo adoptado por la mayoría prevista en el artículo 20, d), del Estatuto del Consejo de Europa y por unanimidad de los representantes de los Estados contratantes que tengan el derecho a formar parte del Comité.

[305] ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, p. 154; ESTADELLA YUSTE, *La protección de la intimidad frente a la transmisión internacional de datos personales*, pp. 65-66.

representantes de las Comunidades Europeas.[306] Para su confección se tomaron en consideración tanto las Resoluciones 73 (22) y 74 (29) del propio Consejo, como también las «orientaciones» de las primeras legislaciones nacionales europeas sobre la materia.[307]

El Convenio señala que su objeto es garantizar a las personas físicas el respeto de su derecho a la vida privada con respecto al tratamiento automatizado de los datos de carácter personal.[308] Una parte de la doctrina considera que el objeto del Convenio sería el derecho a la vida privada y no el reconocimiento del derecho a la protección de datos personales. Así, Ruíz Miguel, señala que «aunque se ha buscado en este Convenio el fundamento para el reconocimiento del derecho a la protección de datos personales lo cierto es que el derecho a la vida privada constituye el único objeto de desarrollo del texto».[309] No obstante, si se examina el Convenio en su conjunto y se revisa la Memoria Explicativa del mismo, es claro que el fin del Convenio es «reforzar la protección de datos».[310]

El otro objetivo (subordinado) del Convenio, sería «la libre circulación de la información», es decir, liberalizar la transferencia de datos personales. Ello se desprende del preámbulo del propio Convenio, donde reconoce «la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos».[311] Por tanto, el respeto y protección de los datos

[306] María del Carmen GUERRERO PICÓ, *El Impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal* (Thomson Civitas, 2006), p. 34; Emilio GUICHOT REINA, *Datos personales y administración pública* (Navarra: Thomson Civitas, 2005), p. 29.

[307] Cfr. El Informe Explicativo del Convención para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal. Disponible en línea en la web del Consejo de Europa: *http://conventions.coe.int/Treaty/en/Reports/Html/108.htm* [consulta: 9.7.2013]

[308] El artículo 1 del Convenio nº 108, titulado *objeto y fin*, dispone que: «El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona».

[309] Cfr. Carlos RUÍZ MIGUEL, «El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea», en *La Carta de Derechos Fundamentales de la Unión Europea: una perspectiva pluridisciplinar* (Valencia: Fundación Rei Afonso Henriques - Tirant Lo Blanch, 2003), pp. 173-210; Ricard MARTÍNEZ MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa* (Madrid: Thomson-Civitas, 2004), p. 161.

[310] Cfr. Memoria Explicativa Convenio 108, parte 1. En el mismo sentido, véase Gregorio GARZÓN CLARIANA, «La protección de los datos personales y la función normativa del Consejo de Europa», *Revista de Instituciones Europeas*, 1981, pp. 15-16.

[311] Gregorio GARZÓN, señala al respecto que «Una interpretación sistemática del Convenio hace aparecer, como objetivo subordinado, el de la liberalización *de iure* de las corrientes de datos personales

personales, debe armonizarse con la libre circulación de los mismos entre los Estados Miembros. Para ello, el Convenio establece un estándar mínimo de protección, ampliable por las legislaciones nacionales. Este estándar mínimo conlleva una serie de derechos instrumentales y principios básicos que las partes deberán tener en cuenta necesariamente a la hora de adoptar en su derecho interno las medidas que hagan efectiva la protección de los datos personales. De esta forma, se logra el objetivo final del Convenio de resguardar los datos personales, como una forma de cautelar el derecho a la vida privada, estableciendo principios esenciales, derechos y garantías mínimas para ello, con el fin de liberalizar la circulación de la información (datos) entre los Estados Miembros.[312]

En cuanto a su ámbito de aplicación, el Convenio no viene limitado *ratione loci* a los territorios europeos, ya que se puede extender su aplicación a otras áreas geográficas (artículo 24); ni tampoco se circunscribe sólo a los Estados Miembros del Consejo, por cuanto el Comité de Ministros tiene la facultad de invitar a otros Estados a adherirse al Convenio (artículo 23.1).[313] Es por ello que se optó por el término «Convención», en vez de «Convención europea». Esta postura aperturista le confiere al Convenio nº 108 una vocación universal en el ámbito de la protección de datos.[314]

En cuanto a su estructura, el Convenio se articula con un preámbulo y 27 artículos, estos últimos, distribuidos en 7 Capítulos. Las partes principales del Convenio son tres: los principios y criterios básicos para la protección de datos: licitud y lealtad, exactitud, finalidad, acceso de la persona interesada, no discriminación y seguridad

---

entre los Estados partes. El Preámbulo, tras recordar o "la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados", reafirma el compromiso de los Estados signatarios "en favor de la libertad de información sin consideración de fronteras", en una alusión apenas velada al artículo 10 del Convenio Europeo de Derechos Humanos. El Convenio no ignora, pues, ese "derecho de comunicarse" en el que se ha visto «una de las manifestaciones del *ius communicationis*». Cfr. Ibid., p. 16.

[312] En el mismo sentido, véase ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, p. 155; ESTADELLA YUSTE, *La protección de la intimidad frente a la transmisión internacional de datos personales*, p. 66; Álvaro SÁNCHEZ BRAVO, *La protección del derecho a la libertad informática en la Unión Europea* (Sevilla: Universidad de Sevilla, 1998), p. 79. También resultan ilustrativos al respecto, los Considerandos del Convenio, así como su Memoria Explicativa.

[313] Como ejemplo, se puede mencionar la República Oriental del Uruguay, que ratificó el Convenio 108 de 1981 y su Protocolo Adicional de 2001, el 10 de abril de 2013 y que entrará en vigor en su territorio el 1 de agosto de 2013. Cfr. la Ley 19.030, publicada en el Diario Oficial de Uruguay con fecha 07.01.2013.

[314] Cfr. Los numerales 19 y 24 del Informe Explicativo del Convenio nº 108. En el mismo sentido véase GARZÓN CLARIANA, «La protección de los datos personales y la función normativa del Consejo de Europa», p. 16.

(capítulo II); disposiciones relativas a los flujos transfronterizos de datos (capítulo III) y la cooperación y ayuda mutua entre las partes contratantes (capítulo IV).

Sobre los principios, se ha planteado que el núcleo del Convenio nº108, sería la «calidad de los datos» (art. 5), a partir del cual se estructuraría, a su vez, el resto de normas y principios que inspiran el Convenio. Los principios derivados de la calidad de los datos, serían los de veracidad, seguridad y finalidad. Por su parte, los derechos de acceso, rectificación y cancelación, constituirían «garantías complementarias» a los principios señalados, a favor de los afectados.[315]

Uno de los puntos más criticados por la doctrina al Convenio 108, fue que éste sólo estableció normas para la transferencia (flujos) de datos entre los Estados que suscriban el acuerdo, omitiendo cualquier regulación sobre las transferencias de datos desde un Estado miembro a un tercer Estado.[316]

Para las transferencias de datos realizadas entre los Estados que suscriban el acuerdo, se estableció como regla general, que los Estados no pueden colocar ningún tipo de objeción a las transferencias internacionales de datos. Es decir, se establece como principios general, la libre circulación de los datos personales dentro del espacio físico que comprenden los Estados Miembros que han suscrito el Convenio.[317] Excepcionalmente, un Estado podría establecer limitaciones a la transferencia de datos a otro Estado parte del Convenio, pero sólo cuando se trate de categorías de datos especiales que estén sometidos a una legislación específica.[318] Esta excepción se establece en función de la naturaleza de los datos que se quieren transferir. Así por ejemplo, si en un Estado los datos sensibles o especialmente protegidos[319] poseen una protección adicional, no podrían transferirse a otro Estado parte, a menos que éste ofreciera un nivel de protección equivalente. La otra situación de excepción pretende

[315] Cfr. GUICHOT REINA, *Datos personales y administración pública*, pp. 30-32.

[316] Por todos, véase PAVÓN PÉREZ, «La protección de datos personales en el Consejo de Europa: el Protocolo Adicional al Convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales»; GARZÓN CLARIANA, «La protección de los datos personales y la función normativa del Consejo de Europa», p. 16.

[317] Artículo 12.1 y 2.

[318] Artículo 12.3.a

[319] El artículo 6 del Convenio señala entre ellos, los que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, y los datos de carácter personal referentes a condenas penales.

evitar que, mediante la triangulación de datos, se burle la legislación del país de procedencia de los datos.[320]

Como se señaló, una de las grandes críticas que le formuló la doctrina al Convenio 108, fue precisamente no regular adecuadamente la transferencia de datos desde los Estados parte del Convenio hacía terceros Estados.[321] Dicha falencia fue corregida el año 2001, mediante un Protocolo Adicional al Convenio, que se dedica a regular dos de los aspectos más débiles de la Convención 108: las autoridades de control y la transferencia internacional de datos a terceros Estados.[322] Sobre este último punto, el Protocolo Adicional estableció como regla general la prohibición de dichas transferencias cuando el Estado u organización internacional de destino de los datos no posea un nivel adecuado de protección.[323] Como se puede apreciar, la condición básica para permitir la transferencia internacional de datos personales desde un país miembro del Consejo de Europa a un tercer Estado u organización internacional que no sea miembro del mismo, es que éstos posean un «nivel adecuado de protección».[324]

No obstante, la realidad impone la necesidad de atenuar el principio general, reconociendo a los Estados parte del Convenio la posibilidad de autorizar transferencias de datos personales a terceros países u organizaciones internacionales que no posean un nivel adecuado de protección en dos supuestos: si el derecho interno del país de origen de los datos así lo establece a causa de «intereses concretos» de la persona afectada (v.g. celebración de un contrato, algún procedimiento médico, entre otros.), o «intereses legítimos», especialmente los de carácter público (v.g. seguridad nacional, seguridad pública, etc.).[325] Por último, también se permite la transferencia a Estados que no garantizan un nivel adecuado de protección si se prevén las «suficientes garantías», que

[320] Artículo 12.3.b

[321] Por todos, véase Gregorio GARZÓN CLARIANA, «La protección de los datos personales y la función normativa del Consejo de Europa», *Revista de Instituciones Europeas*, Vol. 8, nº 1, enero-abril, 1981, p. 16.

[322] Cfr. Protocolo Adicional del Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos. Celebrado en Estrasburgo, el 8 de noviembre de 2001.

[323] Artículo 2.1: «Cada Parte preverá que la transferencia de datos personales a un destinatario sometido a la competencia de un Estado u organización que no es Parte del Convenio se lleve a cabo únicamente si dicho Estado u organización asegura un adecuado nivel de protección»

[324] Sobre qué se entiende por nivel adecuado de protección, véase *infra* apartado 1.4 del capítulo sexto de este trabajo.

[325] Artículo 2.2.a)

pueden resultar, en particular, de cláusulas contractuales por parte del responsable del tratamiento o responsable de la transferencia. Dichas garantías se estimarán adecuadas por las autoridades competentes de conformidad con el derecho interno.[326]

Respecto a las «excepciones» al ejercicio de los derechos de la persona concernida, el Convenio 108 sigue la misma línea de las previsiones consagradas en el artículo 8.2 CEDH.[327] Es decir, se permiten en la medida que lo prevea una ley interna (en este caso del Estado suscriptor del Convenio 108) que constituya una medida necesaria en una sociedad democrática y que persiga fines de interés general. Se señalan como fines de interés general en el Convenio, por una parte, la protección de la seguridad del Estado, de la seguridad pública, los intereses monetarios del Estado y la represión de infracciones penales[328]; y por otra parte, la protección de la persona concernida y de los derechos y libertades de otras personas.[329] También, se consagra en el mismo artículo que los Estados podrán prever por ley «restricciones» en el ejercicio de los derechos acceso, rectificación y cancelación para los ficheros automatizados de datos de carácter personal que se utilicen con fines estadísticos o de investigación científica, cuando no existan manifiestamente riesgos de atentado a la vida privada de las personas concernidas.[330]

Es probable que el Convenio admita con cierta generosidad la posibilidad de establecer excepciones y restricciones a la normativa protectora, posiblemente como contrapartida de la prohibición total de presentar «reservas».[331] Es por ello que cobra importancia, como ya lo planteamos en el estudio del artículo 8 del CEDH, determinar en qué términos debe entenderse que concurren los tres requisitos —previsión en una ley interna, sociedad democrática y fines de interés general— para poder limitar este derecho, lo que se ha denominado «test democrático de restricción de derechos».[332]

---

[326] Artículo 2.2.b)
[327] Al respecto véase *supra*, apartado 1 de éste Capítulo.
[328] Artículo. 9.2.a
[329] Artículo 9.2.b
[330] Artículo 9.3
[331] En este sentido, véase GARZÓN CLARIANA, «La protección de los datos personales y la función normativa del Consejo de Europa», p. 20.
[332] Para un análisis detallado sobre el tema, véase Mónica ARENAS RAMIRO, «El derecho a la protección de datos personales: de la jurisprudencia del TEDH a la del TJCE», en *Constitución y democracia: 25 años de Constitución democrática en España : (actas del congreso celebrado en Bilbao los días 19 a 21 de noviembre de 2003)*, ed. Miguel A. GARCÍA HERRERA, vol. 1 (Bilbao: Servicio Editorial de la Universidad del País Vasco, 2005), pp. 575-588; Teresa FREIXES SANJUÁN, «La

Una de los grandes aportes del Convenio nº 108, fue otorgar fuerza obligatoria a los principios generales de la protección de datos establecidos en las Resoluciones (73) 22 y (74) 29.[333] Como todo Convenio legalmente celebrado, el Convenio 108 es jurídicamente vinculante para los Estados que lo han suscrito y su incumplimiento lleva aparejada sanciones y responsabilidades en el ámbito internacional para el Estado que lo vulnere. La obligación principal de los Estados que lo suscriben sería incorporar a su derecho nacional, por la vía prevista en la Constitución respectiva, los principios, derechos y obligaciones que establece el Convenio, con el objeto de cautelar adecuadamente el derecho a la vida privada de sus ciudadanos en relación con los tratamientos de datos que se realicen, tanto por entes públicos como privados.

Vinculado a su fuerza obligatoria, uno de los problemas que se suscitó fue que después de la ratificación respectiva del Convenio, los Estados no desarrollaron legislativamente el contenido del Convenio.[334] Una parte de la doctrina, se inclinó por su falta de eficacia directa, señalando la necesidad de una norma en el derecho interno que desarrolle los principios contenidos en el Convenio. Con esta interpretación, el Convenio carecería de eficacia directa en el sentido material de su invocabilidad inmediata por un particular ante un juez. Otra parte de la doctrina, defendió la eficacia directa del Convenio y la posibilidad de invocarlo directamente por los ciudadanos en la tutela de sus derechos.[335] Creemos que esta última interpretación en la correcta, ya que de lo

---

protección de los datos automatizados por el Tribunal Europeo de Derechos Humanos», en *Encuentros sobre Informática y Derecho*, ed. Miguel DAVARA RODRIGUEZ (Pamplona: Aranzadi, 1998); María del Carmen GUERRERO PICÓ, *El Impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal* (Thomson Civitas, 2006), pp. 37-38.

[333] María LÁZPITA GURTUBAN, "Análisis comparado de las legislaciones sobre protección de datos de los Estados Miembros de la Comunidad Europea", *Informática y derecho: Revista iberoamericana de derecho informático*, 1994, p. 405; ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, p. 155.

[334] En el caso de España, ello dio pie a una discusión a nivel doctrinario y a un pronunciamiento del Tribunal Constitucional, en relación a si el Convenio poseía el carácter de *self-executing*, es decir, si sus normas eran o no directamente aplicables sin desarrollo legislativo previo. Cfr. STC 254/1993, de 20 de julio. Publicada en el BOE de 18.08.1993. Al respecto véase Julio GONZÁLEZ CAMPOS, Luis SÁNCHEZ RODRIGUEZ, y María Paz ANDRÉS SÁENZ de SANTA MARÍA, *Curso de Derecho Internacional Público*, 8a ed., 3a en Civitas (Madrid: Thomson-Civitas, 2003), pp. 280 y ss.

[335] Sobre la posibilidad aplicar directamente el Convenio 108 sin necesidad de desarrollo legislativo, Carlos RUÍZ MIGUEL, señala que «lo preceptos constitucionales que reconozcan derechos fundamentales se interpretan de forma que *no sólo* sea conforme con las demás normas constitucionales, *sino también* con esos convenio internacionales, de suerte que si existiera una interpretación de estas normas conforme con los demás preceptos constitucionales, pero disconforme con esos convenios, dicha interpretación deberá ser rechazada en beneficio de otra que también sea conforme con esos tratados. Los convenios no permiten una interpretación *contra constitutionem*». Cfr. RUÍZ MIGUEL, *El Derecho a la*

contrario, implicaría dejar al arbitrio de los Estados el momento en el cual se hacen efectivos los derechos fundamentales consagrados en Tratados o Convenios suscritos por el propio Estado. En definitiva, los derechos y principios consagrados en el Convenio son de aplicación directa, sin perjuicio del desarrollo normativo que realice de los mismos el Estado parte del Convenio.

Otro aspecto positivo del Convenio, es haber contribuido a la creación de unos estándares básicos de protección, ampliamente asumidos por los legisladores nacionales de los Estados parte.[336] Además, su contenido ha sido recibido, desarrollado y concretado en el ámbito de la Unión Europea, por instrumentos normativos posteriores, como 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 el ámbito específico de la protección de datos personales en el ámbito de la prevención y represión penal la influencia del Convenio 108 es indudable. La mayor parte de los cuerpos normativos dictados en el antiguo tercer pilar comunitario señalan al Convenio 108, como la norma aplicable para determinar el nivel mínimo a garantizar por parte de los Estados Miembros para el tratamiento de los datos personales.[337]

Por último, queremos desatacar que el Convenio 108 sigue hoy plenamente vigente, como lo manifiesta el hecho que en la 31ª Conferencia Internacional de

---

Protección de la Vida Privada en la Jurisprudencia Del Tribunal Europeo de Derechos Humanos, Civitas, Madrid, 1994. En el mismo sentido, Antonio TRONCOSO REIGADA, señala que «es indudable que los Tratados Internacionales válidamente celebrados, una vez publicados oficialmente en España, forman parte del ordenamiento jurídico interno —art. 96.1 CE—, sin necesidad de *interpositio legislatoris*. No hay que olvidar que el propio artículo 4 del Convenio 108 recoge un compromiso de los Estados Miembros de adaptación de la normativa interna al mismo, sin perjuicio de exigir la aplicación directa de sus preceptos y principios». Cfr. TRONCOSO REIGADA, *La protección de datos personales: en busca del equilibrio*, p. 57.

[336] Al respecto véase Diana SANCHO VILLA, op. cit., p. 57 y bibliografía citada por la autora.

[337] A modo de ejemplo, véase la Decisión del Consejo 2002/187/JAI, de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia; la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información; la Decisión Marco 2006/960/JAI del Consejo, desde 18 de diciembre de 2006 sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados Miembros de la Unión Europea; la Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza; la Decisión Marco 2008/978/JAI del Consejo de 18 de diciembre de 2008, relativa al exhorto europeo de obtención de pruebas para recabar objetos, documentos y datos destinados a procedimientos en materia penal y la Decisión Marco 2008/977/JAI de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, DO L 350 de 30.12.2008, p. 4.

Autoridades de Protección de Datos y Privacidad, celebrada el 5 de noviembre de 2009 en la ciudad de Madrid, gran parte los principios contenidos en la Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal, coinciden con el contenido del Convenio 108.[338]

3. LA RECOMENDACIÓN N º R (87) 15, DEL CONSEJO DE EUROPA, QUE REGULA LA UTILIZACIÓN DE DATOS PERSONALES EN EL SECTOR DE LA POLICÍA, COMO BASE JURÍDICA DE FACTO EN LA MATERIA

El Consejo de Europa fue consciente de que era preciso crear un marco normativo común, pero también advirtió la necesidad de reelaborar los principios del Convenio número 108 en función de las especificidades que presentan los distintos sectores que emplean tratamiento de datos de carácter personal.[339] Es por ello que el Convenio 108 ha sido completado por un conjunto de recomendaciones dirigidas a orientar las decisiones normativas nacionales en sectores específicos.[340] Se ha preferido las recomendaciones a los gobiernos antes que una modificación al Convenio 108 o la adopción de protocolos adicionales. Aquellas ofrecen la ventaja de una elaboración, adopción y puesta en práctica más sencilla, ya que sólo basta con que el Comité de Ministros las adopte por unanimidad, pero tienen la desventaja de que no son jurídicamente vinculantes, ya que queda a criterio de cada Estado realizar las adecuaciones normativas en su legislación interna para darles cumplimiento.

---

[338] Sobre la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada el 5 de noviembre de 2009 en Madrid y la Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal, véase *https://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf* [consulta: 26.03.2010].

[339] María del Carmen GUERRERO PICÓ, *El impacto de internet en el derecho fundamental a la protección de datos de carácter personal*, Aranzadi, Navarra, 2006, p. 43.

[340] Algunas de estas Recomendaciones son: nº R (80) 13, de 18 de septiembre, relativa al intercambio de informaciones jurídicas en materia del protección de datos; nº R (81) 1, de 23 de enero, relativa a la reglamentación aplicable a los bancos de datos médicos automatizados; nº R (83) 10, de 23 de septiembre, relativa a la protección de datos de carácter personal utilizados con fines de investigación científica y de estadística; nº R (85) 20, de 25 de octubre, relativa a la protección de datos de carácter personal utilizados con fines de *marketing* directo; nº R (86) 1, de 23 de enero, relativa a la protección de datos de carácter personal utilizados con fines de seguridad social; nº R (87) 15, de 17 de septiembre, dirigida a regular la utilización de datos de carácter personal en el sector de la policía (sometida a tres informes de evaluación, en 1994, 1998 y 2002). El listado completo se puede consultar en la web del Consejo de Europa: *http://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp* [consulta: 10.07.2013]

El Consejo de Europa fue previsor y anunció la creciente utilización de los datos personales y de su tratamiento automatizado en el sector de la policía, como así mismo, de los posibles beneficios obtenidos a través del uso de la informática combinadas con otras técnicas (ADN, datos dactiloscópicos, etc.). También anticipó la posible amenaza a la intimidad de las personas que ello implica y de la necesidad de equilibrar los intereses en juego. Es por ello que se dictó la Recomendación n º (87) 15, del Consejo de Europa, que regula la utilización de datos personales en el sector de la policía (en adelante, la Recomendación (87) 15.[341] Esta tiene por objeto servir de guía para el derecho interno de los Estados Miembros y la práctica policial, en lo relativo a la aplicación de los principios esenciales para la recogida, almacenamiento, uso y comunicación de datos personales con fines policiales, garantizando, a la vez, los derechos relativos a las protección de la intimidad y datos personales de los particulares.[342]

Llama la atención que en el ámbito del Consejo de Europa este instrumento constituya el único texto específico sobre la materia (protección de datos y cooperación policial) respecto del cual se ha llegado a un consenso. Es probable que ello se deba a su naturaleza jurídica de «Recomendación», lo que implica que no es vinculante para los Estados Miembros del Consejo de Europa, sino meramente indicativo de las medidas legales a adoptar, con la finalidad de equilibrar, por un lado, los intereses de la sociedad en la prevención y represión de los delitos y el mantenimiento del orden público, y por otro, los intereses del individuo y su derecho a la intimidad y protección de datos personales.

El marco de referencia de la Recomendación (87) 15 se encuentra dado por las disposiciones de la Convención 108 del Consejo de Europa para la Protección de las personas con respecto al tratamiento automatizado de los Datos Personales, de 28 de enero de 1981, particularmente, lo relativo a las excepciones permitidas en virtud del

[341] Adoptada por el Comité de Ministros el 17 de septiembre de 1987, en la 410 ª sesión de los Ministros

[342] Al respecto véase Emilio ACED FÉLEZ, «La protección de datos en la cooperación policial europea : de la Recomendación (87) 15 al principio de disponibilidad: Título IV. Disposiciones Sectoriales. Cap. I. Ficheros de Titularidad Pública. artículos 22, 23.1 y 24.1»; ESTADELLA YUSTE, *La protección de la intimidad frente a la transmisión internacional de datos personales*, p. 66; Manuel HEREDERO HIGUERAS, «La protección de datos personales en manos de la policía: reflexiones sobre el Convenio de Schengen», en *La protecció de dades personals. Regulació nacional i internacional de la seguridad informàtica* (Barcelona: Cetre d' Investigació de la Comunicació i Universidad Pompeu Fabra, 1993), pp. 29-49.

artículo 9[343]; y las disposiciones del artículo 8 de la Convención para la Protección de los Derechos Humanos, Derechos y las Libertades Fundamentales.[344] Por tanto, debemos entender que la interpretación que se realice de la Recomendación (87) 15 debe ser a la luz de lo que disponen ambos instrumentos a los cual remite.

En cuanto al ámbito de aplicación de la Recomendación (87) 15, este se refiere a la recogida, almacenamiento, uso y comunicación de datos personales con fines policiales que son objeto de procesamiento "automatizado". Es decir, regula el tratamiento, almacenamiento y cesión de datos de carácter personal automatizados por parte de los cuerpos policiales. No obstante lo anterior, la Recomendación permite a los Estados miembros ampliar los principios contenidos en ella a los datos no tratados de forma automatizada, pero con la advertencia de que el procesamiento manual de datos no deberá tener lugar si el objetivo es evitar las disposiciones de la presente Recomendación.[345] También se permite que un Estado miembro pueda ampliar los principios contenidos en la Recomendación a los datos relativos a los grupos de personas, asociaciones, fundaciones, empresas, corporaciones o cualquier otro organismo compuesto directa o indirectamente de las personas, tengan o no personalidad jurídica.[346] Las disposiciones de la Recomendación puedan extenderse, en su caso, a la recogida, almacenamiento y uso de datos personales con fines de seguridad del Estado.[347]

La Recomendación, al igual que el Convenio 108 y Protocolo Adicional, entrega ciertas definiciones de uso frecuente en el mismo. En su mayoría son las mismas que las señaladas en los citados instrumentos. Así, por ejemplo, señala que la expresión «datos personales» abarca cualquier información relativa a una persona física identificada o identificable, agregando que un individuo no se considerará como «identificable» si la identificación requiere una cantidad razonable de tiempo, coste y mano de obra. Asimismo, señala que la expresión «a efectos policiales» abarca todas las tareas que las autoridades de policía deban realizar para la prevención y represión de los delitos y el mantenimiento del orden público. La expresión «órgano competente» (responsable del archivo) denota la autoridad, servicio o cualquier otro organismo público que sea

[343] Al respecto, véase apartado 2 de éste capítulo.
[344] Al respecto, véase apartado 1 de éste capítulo.
[345] Cfr. *Ámbito de aplicación y definiciones,* contenidas en el apéndice a la Recomendación nº R (87) 15.
[346] Ídem.
[347] Ídem.

competente conforme a la ley nacional para decidir sobre la finalidad de un fichero automatizado, las categorías de datos personales que deben ser almacenados y las operaciones que se aplican a ellos.

Los principios básicos que recoge la Recomendación (87) 15, son: el control y la notificación (principio 1); la recopilación de datos (principio 2); el almacenamiento de datos (principio 3); la utilización de los datos de la policía (principio 4); la comunicación de datos (principio 5). Dentro de éste regula, a su vez, la comunicación dentro del sector de la policía, la comunicación a otros organismos públicos, la comunicación a particulares y la comunicación internacional. También regula las solicitudes, condiciones y salvaguardias para la comunicación. La Recomendación, regula la interconexión de los archivos y el acceso en línea a los mismos. Se contempla también la regulación de la publicidad, el derecho de acceso a los archivos de la policía, el derecho de rectificación y derecho de cancelación y/o supresión (principio 6), la duración del almacenamiento y la actualización de los datos (principio 7); y por último, la seguridad de los datos (principio 8).

A pesar del tiempo transcurrido desde su aprobación, la Recomendación sigue teniendo actualmente una importancia innegable para la regulación del tratamiento de datos personales en el ámbito policial. Ello se debe en gran medida, en una primera etapa, a la falta de regulación sobre la materia en la Unión Europea, y luego, una vez aprobada la Decisión Marco 2008/977/JAI[348] (en adelante, DM 2008/977), al limitado ámbito de aplicación de la misma, lo que ha llevado a considerar a la Recomendación (87) 15 como un «estándar *de facto*» para la protección de datos en los tratamientos de datos personales llevados a cabo con finalidad de investigación policial en el ámbito europeo. Ello se ha producido a través de su incorporación como requisito mínimo en varios convenios y decisiones de la UE, tales como Schengen, Europol, Sistema de Información Aduanera o Eurojust.[349]

[348] 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. Publicado en el DOUE L 350/60, de 30 de diciembre de 2008.

[349] ACED FÉLEZ, «La protección de datos en la cooperación policial europea : de la Recomendación (87) 15 al principio de disponibilidad: Título IV. Disposiciones Sectoriales. Cap. I. Ficheros de Titularidad Pública. artículos 22, 23.1 y 24.1», pp. 2-4. En la misma línea, Cristina Dietrich señala que «es significativo en este sentido que, en el ámbito de las políticas de cooperación policial y judicial en materia penal en la Unión Europea, y por lo que respecta a la normativa de protección de datos, vista la dificultad que ha supuesto aprobar la Decisión Marco de protección de datos en este ámbito, los textos legales

Para concluir el apartado, podemos señalar que la labor desarrollada por Consejo de Europa en el ámbito de la protección de datos ha sido innovadora, ya que ha establecido las bases y los principios esenciales que gobiernan este tema, y que se han mantenido hasta la actualidad, con las adecuaciones propias a los nuevos adelantos tecnológicos. A medida que la información y comunicación se desarrollan, se generan nuevas necesidades, incluido el ámbito específico de la protección de datos de carácter personal y la cooperación policial. Pudimos constatar que el único instrumento específico que existía, hasta no hace mucho tiempo, era la Recomendación (87) 15 del Consejo de Europa. Ésta trata de conciliar, por un lado, la necesidad social de prevenir y reprimir los delitos y mantener el orden público, y por otro, el derecho a la intimidad y la protección de los datos personales. A pesar de que dicho instrumento no posee un carácter vinculante, el impacto del mismo sobre el tema específico que tratamos es evidente, como tendremos ocasión de ver en el siguiente apartado, donde veremos cómo la regulación específica dictada en el marco de la Unión Europea hace recepción de gran parte de sus principios.

consolidados de referencia sigan siendo, en cierta medida, el Convenio 108 del Consejo de Europa, de 1981, Y sus textos de desarrollo, así como la Recomendación (87) 15, del Consejo de Europa, relativa al uso de datos personales en el sector de la policía, que recoge principios de actuación en relación con el tratamiento, almacenamiento y cesión de datos por parte de cuerpos policiales. Cfr. Cristina DIETRICH PLAZA, «Las tensiones entre libertad y seguridad en el marco jurídico actual de protección de datos de carácter personal en la Unión Europea», en *Libertad, seguridad y transformaciones del Estado*, ed. Joan Lluís PÉREZ FRANCESCH (Barcelona: Institut de Ciències Polítiques i Socials, 2009), p. 186.

CAPÍTULO QUINTO

NORMATIVA GENERAL DE LA UNIÓN EUROPEA EN MATERIA DE PROTECCIÓN DE DATOS

SUMARIO: INTRODUCCIÓN; 1 TRATADO DE LISBOA Y LA NUEVA BASE JURÍDICA DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS (Artículo 17 TFUE); 1.1. Configuración actual del Tratado de Lisboa como fuente del derecho Europeo; 1.2. Espacio de libertad, seguridad y justicia; 1.3. Programas para consolidar el espacio de libertad, seguridad y justicia; 1.4. Disposiciones relativas a la cooperación policial en materia penal; 1.5. Protección de datos de carácter personal en el ámbito de la cooperación policial en materia penal; 2. CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA; 2.1. CDFUE como fuente del derecho europeo; 2.2. Derecho a la protección de datos como derecho fundamental autónomo; 2.3. Reconocimiento de la CDFUE en el Tratado de Lisboa y su impacto para el derecho fundamental a la protección de datos; 3. LAS DIRECTIVAS EUROPEAS; 3.1. Directiva 95/46/CE y la propuesta de un nuevo Reglamento General; 3.2. Directiva 2006/24/CE. El cuestionamiento a su base jurídica; 3.3. Reglamento 45/2001 relativo al tratamiento de datos personales por las instituciones y los organismos comunitarios.

INTRODUCCIÓN

En el presente capítulo nos proponemos analizar la normativa general actualmente vigente en Europa en materia de protección de datos personales.[350] Partimos este estudio con el Tratado de Lisboa, por la transcendencia que tiene en el cambio de la arquitectura institucional y normativa de la Unión, y que en el ámbito específico del derecho fundamental a la protección de datos se traduce en una nueva base jurídica. Luego se analizan las principales directivas sobre la materia y su

[350] Sobre la protección de datos personales en la Unión europea existe una abundante bibliografía, por todos véase ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*; Mónica ARENAS RAMIRO, «Integración europea y protección de datos personales. Las garantías específicas del derecho a la protección de datos personales», *Anuario de la Facultad de Derecho*, 2005 de 2004; Mónica ARENAS RAMIRO, «La protección de datos personales en los países de la Unión Europea», *Revista jurídica de Castilla y León* n.º 16 (2008): pp. 113-168; Abel TELLEZ AGUILERA, *La protección de datos en la Unión Europea* (Madrid: Edisofer, 2002); GUERRERO PICÓ, *El Impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, pp. 55-134; Lucrecio REBOLLO DELGADO, *Vida privada y protección de datos en la Unión Europea* (Madrid: Dykinson, 2008), pp. 103-133; TRONCOSO REIGADA, *La protección de datos personales: en busca del equilibrio*, pp. 56-63.

vinculación con el tratamiento de datos personales en el ámbito policial, poniendo especial énfasis en la nueva Propuesta de Reglamento general de protección de datos personales COM(2012) 11 final, del Parlamento Europeo y del Consejo. También veremos los fallos del Tribunal de Justicia de la Comunidades Europeas respecto de la Directiva 2006/24, dónde primero se cuestionó la utilización de la base jurídica utilizada para realizar labores propias del antiguo tercer pilar comunitario, así como la última sentencia dictada en abril de 2014 que finalmente deja sin efecto dicho instrumento por su evidente vulneración a las disposiciones de la Carta de Derechos Fundamentales de la Unión Europea. Por último, hacemos referencia al Reglamento 45/2001 relativo al tratamiento de datos personales por las instituciones y los organismos comunitarios.

1. TRATADO DE LISBOA Y LA NUEVA BASE JURÍDICA DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS

1.1. Principales cambios que introduce el Tratado de Lisboa

El Tratado de Lisboa, que entró en vigor el 1 de diciembre de 2009, modifica por un parte el Tratado de la Unión Europea y, por otra, el Tratado constitutivo de la Comunidad Económica Europea, que pasa a denominarse Tratado de Funcionamiento de la Unión Europea (art.1 TUE).[351] Dentro de los grandes cambios que introduce el

[351] Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea. Publicado en el D.O. n° C 306 de 17 de diciembre de 2007. Disponible en *eur-lex.europa.eu/*. [Consultado el 30.9.2013]. Sobre el Tratado de Lisboa véase, entre otros, Francisco ALDECOA LUZÁRRAGA y Mercedes GUINEA LLORENTE, *La Europa que viene: el Tratado de Lisboa*, 2° ed. (Madrid: Marcial Pons, 2010); José Enrique AYALA, «Lisboa, por fin: el tratado abre una nueva era en la UE», *Política exterior* 24, n.º 133 (2010), pp. 13-20; Francisco BALAGUER CALLEJÓN, «El Tratado de Lisboa en el diván. Una reflexión sobre estatalidad, constitucionalidad y Unión Europea», *Revista española de derecho constitucional* 28, n.º 83 (2008), pp. 57-92; Antonio D'Atena, «La Constitución oculta de Europa (antes y después de Lisboa)», *Revista de derecho constitucional europeo* n.º 13 (2010), pp. 17-46; Jesús DE LA IGLESIA GARCÍA, «La entrada en vigor del Tratado de Lisboa», *RUE: Revista universitaria europea* n.º 12 (2010), pp. 45-60; Excmo Sr D. Javier ROJO GARCÍA et al., «El Tratado de Lisboa: la salida de la crisis constitucional» (2008); Gurutz JÁUREGUI BERECIARTU y Juan Ignacio UGARTEMENDÍA ECEIZABARRENA, «Europa en el lecho de Procusto: de la Constitución europea al Tratado de Lisboa», *Revista Vasca de Administración Pública. Herri-Arduralaritzako Euskal Aldizkaria* n.º 79 (2007), pp. 105-126; José MARTÍN Y PÉREZ DE NANCLARES y Mariola URREA CORRES, *Tratado de Lisboa* (Madrid: Real Instituto Elcano & Marcial Pons., 2008); Lucía MILLÁN MORO, «El ordenamiento jurídico comunitario: del Tratado Constitucional al Tratado de Lisboa», *Revista de Derecho Comunitario Europeo* 14, n.º 36 (2010), pp. 401-438; «El Tratado de Lisboa entra en vigor», *Razón y fe: Revista hispanoamericana de cultura* 260, n.º 1334 (2009), pp. 339-346.

Tratado de Lisboa, se encuentran el aumento de la integración política entre los Estados miembros y las instituciones europeas, al simplificar y determinar los respectivos ámbitos de competencia.[352] Asimismo, se incrementan los ámbitos de codecisión entre el Parlamento y el Consejo, se crean nuevos órganos permanentes y se flexibilizan las condiciones para la europeización de normas y políticas públicas. También, se destaca el cambio en la forma de tomar las decisiones, ya que estas podrán ser adoptadas por mayoría cualificada y no como hasta ahora por unanimidad del Consejo. No obstante, los Estados miembros mantienen la posibilidad de emprender iniciativas legislativas sobre cooperación policial operativa, justicia penal y cooperación administrativa, siempre y cuando las respalde una cuarta parte del total de países.[353]

También es importante resaltar que el Tribunal de Justicia de la Unión Europea, será competente en relación a los instrumentos legales que se suscriban con posterioridad al Tratado de Lisboa. Respecto de los actos legislativos anteriores al Tratado, el TJUE no tendrá competencia durante los cinco primeros años de vigencia del Tratado.[354] Por último, el artículo 6 del TUE, consagra, por una parte que la Carta de los Derechos Fundamentales de la Unión Europea tiene el mismo valor jurídico que los Tratados, y por otra, que La Unión se adherirá al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Los derechos fundamentales que ésta consagra y las tradiciones constitucionales comunes de los Estados miembros, pasan a constituir principios generales del derecho de la Unión.[355]

---

[352] Cfr. El Título I (Categorías y Ámbitos de Aplicación) del Tratado de la Unión Europea. Sobre el reparto de poderes y las competencias en el Tratado de Lisboa, véase Stelio MANGIAMELI, «El diseño institucional de la Unión Europea después del Tratado de Lisboa», http://www.ugr.es/~redce/REDCE15/articulos/10SMangiameli.htm#resumen [consultado el 12.07.2013].

[353] Cfr. artículo 20 del Título IV «Disposiciones sobre las cooperaciones reforzadas» del TUE. Al respecto véase el libro monográfico de BENEYTO PÉREZ, José María, MAILLO GONZÁLEZ-ORÚS JERÓNIMO, y BECERRIL ATIENZA Belén, eds., *Unidad y flexibilidad en el futuro de la Unión Europea: el desafío de las cooperaciones reforzadas* (Universidad San Pablo-CEU, 2010); y en particular del mismo libro a Belén BECERRIL ATIENZA, «La regulación de la cooperación reforzada y su reforma en Lisboa: hacia un modelo de diferenciación más cercano al método comunitario», en (2010), pp. 15-34.

[354] Cfr. Sección 5° del Capítulo I del TFUE; Protocolo (n° 3) «Sobre el Estatuto del Tribunal de Justicia de la Unión Europea». Sobre el Tribunal de Justicia de la Unión Europea, véase Dámaso Ruíz-Jarabo y Colomer, «El Tribunal de Justicia de la Unión Europea en el Tratado de Lisboa», *Noticias de la Unión Europea* n.º 291 (2009), pp. 31-40.

[355] Sobre la Carta de Derecho Fundamental de la Unión Europea y el Tratado de Lisboa, véase Manuel LÓPEZ ESCUDERO et al., "Carta de los Derechos Fundamentales de la Unión Europea", 2008; Teresa PAREJO NAVAJAS, "La Carta de los derechos fundamentales de la Unión Europea", *Derechos y Libertades: Revista de filosofía del derecho y derechos humanos*, enero de 2010. Silvio GAMBINO, "Jurisdicción y justicia entre Tratado de Lisboa, Convenio Europeo de Derechos Humanos y ordenamientos nacionales", *Revista de derecho constitucional europeo*, nº 13 (2010): pp. 83–120. Cristina BLASI CASAGRAN, «La protección de los Derechos Fundamentales en el Tratado de Lisboa»,

Lo anterior, impacta también en la protección de datos en el ámbito de la cooperación judicial y policial en materia penal, ya que el artículo 6 del Tratado de la Unión Europea, es aplicable a la cooperación judicial y policial. Por tanto, para la adecuada interpretación de las normas sobre protección de datos en lo vinculado a la prevención y represión penal, debemos tener presente tanto el CEDH, como las tradiciones constitucionales comunes de los Estados miembros.[356]

1.2. El espacio de libertad, seguridad y justicia

El espacio de libertad, seguridad y justicia, fue creado por el Tratado de Maastricht (1992) y desarrollado en los programas de Tampere (1999-2004), La Haya (2004-2009) y Estocolmo (2010-2014). Antes de la reforma del Tratado de Lisboa, su base jurídica se encontraba en el Título IV del Tratado Constitutivo de la Comunidad Europea que cubría todos los ámbitos, a excepción de la cooperación policial y judicial penal, regulada por el Título VI del Tratado constitutivo de la Unión Europea. Así pues, el espacio de justicia, libertad y seguridad correspondía a la vez al régimen comunitario (antiguo primer pilar) y al régimen intergubernamental (antiguo tercer pilar). Con la entrada en vigor del Tratado de Lisboa, se suprime la estructura de pilares, tal como se habían configurado formalmente a partir del Tratado de Ámsterdam (1997), y gestados previamente a partir del Tratado de Maastricht, por lo que los actos de la Unión, en el ámbito de la cooperación policial y judicial en asuntos penales, pasa a formar parte del espacio de libertad, seguridad y justicia.

La europeización del extinto tercer pilar comunitario, implica que las orientaciones estratégicas sobre la materia serán adoptadas por el Consejo, por medio

---

Institut Universitari d' Estudis Europeus 51, Quaderns de treball (octubre de 2010); Joan Lluís PÉREZ FRANCESCH, *La cooperación policial y judicial en el Tratado de Lisboa, entre la europeización y las reservas estatales,* ponencia presentada al VIII Congreso de la Asociación de Constitucionalistas de España, San Sebastian, 4 y 5 de febrero de 2010, *http://www.acoes.es/congresoVIII/documentos/PonenciaJLPerezFrancesch.pdf*

[356] Al respecto véase Joan Lluís PÉREZ FRANCESCH, «La cooperación policial y judicial en el Tratado de Lisboa, entre la europeización y las reservas estatales», en *Derecho constitucional europeo. Actas del VIII Congreso de la Asociación de Constitucionalistas de España.*, ed. Juan Ignacio Ugartemendía Eceizabarrena y Gurutz Jáuregui Bereciartu (Valencia: Tirant lo Blanch, 2011), pp. 465-489, http://www.acoes.es/congresoVIII/documentos/PonenciaJLPerezFrancesch.pdf; Joaquín BAYO DELGADO, «La cooperación policial internacional a la luz de la Propuesta revisada de Decisión Marco relativa a la protección de datos», en *La protección de datos en la cooperación policial y judicial* (Pamplona: Aranzadi, 2008), pp. 23-36.

de su programación operativa y legislativa. Los Estados, por medio de sus Parlamentos nacionales, también podrán participar en el proceso de evaluación de las medidas y las actividades llevadas a cabo tanto por Eurojust como por Europol. Ello constituye una manifestación de la finalidad de otorgar una mayor democracia en el nuevo diseño europeo. No obstante, se establece una importante restricción, ya que el TJUE no será competente para comprobar la validez o proporcionalidad de las operaciones efectuadas por la policía u otros servicios con funciones coercitivas de un Estado miembro, ni para pronunciarse sobre el ejercicio de las responsabilidades que incumben a los Estados Miembros respecto del mantenimiento del orden público y de la salvaguardia de la seguridad interior.[357] Sin embargo, esta restricción no afecta a los controles internos que posea cada Estado. Así los tribunales de cada Estado miembro, pueden pronunciarse en última instancia sobre la validez y proporcionalidad de las operaciones llevadas a cabo por las fuerzas y cuerpos de seguridad que tengan como justificación el mantenimiento del orden público y de la salvaguardia de la seguridad interior.

La desaparición de los pilares y, por tanto, la incorporación del ámbito de la cooperación judicial y policial al espacio de libertad, seguridad y justicia, no implica la eliminación de la facultad de los Estados Miembros de emprender iniciativas legislativas, por el contrario, los Estados Miembros mantendrán la posibilidad de emprender iniciativas legislativas sobre cooperación policial, justicia penal o cooperación administrativa, siempre y cuando las respalde una cuarta parte de los mismos. Además, se permite que los Estados Miembros puedan presentar reservas y no seguir la política común. Esto tiene como finalidad, básicamente, superar los bloqueos que se producían antes por la exigencia de la unanimidad en la toma de decisiones. Por tanto, existe una mayor flexibilización en la toma de las decisiones, que algunos autores han llamado «una Europa a la carta».[358] Ello representa un paso adelante en la construcción europea, ya que permite superar el recurso tradicional de la cooperación por medio del método intergubernamental, a través de Tratados y Convenciones entre algunos de los Estados Miembros, que se suscribían precisamente con el fin de saltarse los pasos señalados para lograr acuerdos en cierta materias de interés común, pero que

[357] Artículo 276 TFUE.
[358] Al respecto véase Sergio CARRERA y Florian GEYER, «El Tratado de Lisboa y un Espacio de Libertad, Seguridad y Justicia: Excepcionalismo y Fragmentación en la Unión Europea», *Revista de Derecho Comunitario Europeo*, n. 29, enero-abril 2008, pp. 133-162.

más tarde se incorporaban al ordenamiento jurídico europeo, como ocurrió con los Acuerdos de Schengen y la Convención de Prüm, por nombrar algunos ejemplos. Con el nuevo procedimiento las decisiones del Consejo habrán de ser aprobadas por mayoría cualificada, lo que significa el 55% de los Estados Miembros que reúnan como mínimo el 65% de la población europea. Es lo que se conoce como doble mayoría. Se necesitará un mínimo de cuatro Estados para formar una minoría de bloqueo.

Otra manifestación de la mayor flexibilidad en el proceso de construcción europea que conlleva el Tratado de Lisboa, es la posibilidad de algunos Estado de «excepcionarse» en el cumplimiento de las disposiciones europeas. Un caso emblemático se encuentra en los casos de Reino Unido e Irlanda. Estos Estados, no aplican las disposiciones sobre la cooperación judicial y policial en materia penal, gracias un Protocolo adicional al Tratado de Lisboa.[359] También se flexibiliza la iniciativa para la adopción de actos en el ámbito de la cooperación policial y judicial, ya que la Comisión comparte la iniciativa con los Estados, siempre que la propuesta sea presentada por un mínimo representado por la cuarta parte de los Estados miembros. A los Estados que no le interese regirse por un determinado acto que pretenda dictarse en el ámbito regulado por los Capítulos 4 y 5 del Título V del TFUE, pueden «obstaculizar» innovaciones que se pretendan introducir si a juicio de un Estado miembro la misma «afecta a aspectos fundamentales de su sistema de justicia penal», solicitando que la cuestión se remita al Consejo Europeo.

Por último nos interesa remarcar, como lo afirma el TFUE, que la Unión constituye un espacio de libertad, seguridad y justicia dentro del respeto de los derechos fundamentales y de los distintos sistemas y tradiciones jurídicas de los Estados Miembros.[360] Por tanto, las medidas legislativas que se adopten en la consagración de dicho espacio, debe respetar los derechos fundamentales de las personas que se encuentran dentro de la Unión. Así por ejemplo, dentro de las políticas de combate contra el terrorismo y las formas graves de delincuencia organizada, la policía puede recurrir al uso de las nuevas TIC, pero respetando los derechos y

[359] Protocolo (nº 21) sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia.
[360] Artículo. 67.1

libertades fundamentales de las personas, y en particular, su privacidad y datos personales. Al respecto se ha señalado que la exigencia del respeto a los derechos fundamentales en esa labor, en un «auténtico caballo de batalla de los tiempos actuales».[361]

1.3. Los programas para consolidar el espacio de libertad, seguridad y justicia

Los Programas del Consejo Europeo, son un marco general de acción que se han fijado los Estados Miembros de la Unión Europea para consolidar el espacio de libertad, seguridad y justicia. Tienen su origen en el Consejo Europeo de Támpere, que dio origen al Programa plurianual del mismo nombre (1999-2004)[362], continuó con el Programa de La Haya (2005-2009)[363], y actualmente nos encontramos en la última fase del Programa de Estocolmo (2010-2014).[364] Estos programas, permiten a la Unión europea fijarse objetivos comunes y coordinar las acciones en las materias que caben dentro de su ámbito. Su importancia para el estudio de la protección de los datos personales en el ámbito de la cooperación policial y judicial en Europa, es que determinan la **orientación** de la futura legislación que ha de dictarse sobre la materia, por lo que nos sirve de referente a la hora de realizar una interpretación sistemática de la misma.

En el Programa de Támpere, se establecieron las bases para una política común de asilo e inmigración, preparando la armonización de los controles fronterizos, mejorado la cooperación policial, y se avanzó sustancialmente en los trabajos preliminares para la cooperación judicial sobre la base del principio de reconocimiento mutuo de resoluciones judiciales y de sentencias. Un punto de inflexión y de orientación de estos programas se produce con posterioridad a los atentados terroristas cometidos en

[361] Ibídem., p. 2. En la misma línea, los principios rectores de la Unión Europea dispone que «La Unión se fundamenta en los valores de respeto de la dignidad humana, libertad, democracia, igualdad, Estado de Derecho y respeto de los derechos humanos, incluidos los derechos de las personas pertenecientes a las minorías». Cfr. Artículo 2 TUE.

[362] Consejo Europeo celebrado en el ciudad finlandesa de Támpere, los días 15 y 16 de octubre de 1999, que establece las bases para la creación de un espacio de libertad, seguridad y justicia en la Unión Europea

[363] El Programa de la Haya: Consolidación de la Libertad, la Seguridad y la Justicia en la Unión Europea, (2005/C 53/01). Publicado en DOUE nº C 53/1 con fecha 03.03.2005.

[364] Programa de Estocolmo: Una Europa abierta y segura que sirva y proteja al ciudadano. Publicado en el DOUE nº C 115/1 con fecha 04.05.2010.

Nueva York el 11 de septiembre de 200, Madrid el 11 de marzo de 2004 y Londres el 7 de julio de 2005. A partir de estos hechos, la seguridad de la Unión y de los Estados Miembros pasa a tener un carácter prioritario en las políticas que se desarrollaron, dándole especial énfasis a la prevención y represión del terrorismo, pero sin descuidar otros ámbitos importantes, como la delincuencia organizada, la migración ilegal, la trata y la introducción clandestina de seres humanos en los países de la Unión.[365]

El Programa de la Haya parte formulando la siguiente pregunta ¿cómo reforzar el espacio de libertad, seguridad y justicia en la Unión Europea? La Comisión responde a esta pregunta estableciendo 10 prioridades para el periodo 2004-2009, que constituye a su vez el plan de acción a desarrollar.[366] En síntesis, estas prioridades buscan establecer políticas de acción común, aproximando las legislaciones de los Estados Miembros, en materias de especial importancia, como los son, entre otras, la lucha contra el terrorismo, la inmigración ilegal y la trata de seres humanos; desarrollar un sistema común de asilo e inmigración, mejorar el acceso a la justicia y ampliar la cooperación judicial y policial. Sobre este último punto, se pretende encontrar el equilibrio adecuado entre la protección de la vida privada y la seguridad al compartir información, en otras palabras, se pretende encontrar un equilibrio en el respeto de los derechos fundamentales, y particularmente en el respeto a la privacidad y los datos personales con la necesidad de disponibilidad de información, por parte de las fuerzas y cuerpos de seguridad en la lucha contra el terrorismo, el tráfico ilícito de drogas y otras formas graves de delincuencia organizada internacional**.**

Actualmente, se está desarrollando el Programa de Estocolmo (2010-2014). Este programa de trabajo estratégico plurianual en el ámbito de la libertad, la seguridad y la justicia, establece las prioridades en la actuación de la Unión Europea en estos cinco años. En la misma línea que sus predecesores, pone al ciudadano en el centro de la actuación de la Unión y aborda, entre otras cosas, cuestiones relativas a la ciudadanía, la

[365] Manifestaciones de estas políticas son, la Decisión Marco 2002/475/JAI, de 13 de junio de 2002, sobre la lucha contra el terrorismo. Publicada en el DOUE nº L 164 de fecha 22.06.2002; y la Decisión Marco 2008/919/JAI del Consejo, de 28 de noviembre de 2008, por la que se modifica la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo. Publicada en el DOUE nº L 330 de fecha 9.12.2008.

[366] Comunicación de la Comisión al Consejo y al Parlamento Europeo, de 10 de mayo de 2005, «Programa de La Haya: Diez prioridades para los próximos cinco años. Una asociación para la renovación europea en el ámbito de la libertad, la seguridad y la justicia». COM (2005) 184 final. Publicado en el DOUE nº C 236 de 24.09.2005.

justicia y la seguridad, así como el asilo, la migración y la dimensión exterior de la justicia y los asuntos de interior. La seguridad informática pasa a ser un tema prioritario en este programa. Se pretende que la Unión Europea, cuente con un único sistema de protección de datos personales que incluya la certificación europea para las tecnologías, productos y servicios que protejan la intimidad. De la lectura del Programa de Estocolmo podemos concluir que se trata de conciliar, la necesidad del intercambio de datos personales, dando cumplimiento al principio de disponibilidad consagrado en el Programa de la Haya, con el debido respeto de la vida privada de las personas.

Cabe recordar que el derecho al respeto de la vida privada y el derecho a la protección de los datos personales de los ciudadanos están inscritos en la Carta de los Derechos Fundamentales (artículos 7 y 8), por tanto, la Unión debe ponderar estos derechos frente a la creciente necesidad de intercambio de información en funciones de prevención y represión de infracciones penales. La forma de lograrlo es desarrollando una estrategia global para proteger los datos dentro de la Unión, y en sus relaciones con otros países y organismos internacionales.

Esta estrategia debe respetar los principios, derecho y obligaciones que se consagran tanto en los instrumentos de la Unión (v.g. la Decisión Marco 2008/977/JAI), como en el Consejo de Europa (Convenio nº 108 de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal). Éste último, sigue siendo la base para articular o determinar el nivel mínimo de protección de los datos personales en el ámbito de la cooperación policial, cuando se realicen tratamientos de datos personales en la prevención y represión de ilícitos. Esto es así, por las insuficiencias y falencias de la Decisión Marco dictadas para regular los datos personales tratados en el antiguo tercer pilar comunitario.[367] Haciéndose eco de una de las principales críticas formuladas a la Decisión Marco 2008/977/JAI del Consejo, el Programa de Estocolmo manifiesta la necesidad de crear un marco legislativo coherente de la Unión en materia de transferencia de datos personales a terceros países con fines policiales.[368] En esta línea se presentó, en enero de 2012, la

[367] Sobre las críticas a la Decisión Marco 2008/977/JAI del Consejo, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial, véase el apartado final del capítulo III de este trabajo.
[368] Véase el Programa de Estocolmo, apartado 7.4. sobre "Acuerdos con terceros países", p. 35

propuesta de Directiva en el ámbito de prevención y represión penal que deroga y sustituye a la Decisión Marco 2008/977/JAI.[369]

1.4. Disposiciones relativas a la cooperación policial en materia penal

En el ámbito específico de la cooperación policial, el Tratado de Funcionamiento de la Unión Europea busca la colaboración entre los servicios de policía, de aduanas y otros servicios con funciones coercitivas especializados en la prevención, detección e investigación de infracciones penales de los Estados Miembros.[370] Contempla la posibilidad de que, con arreglo al procedimiento legislativo ordinario, se puedan adoptar medidas relacionadas con: a) la recogida, almacenamiento, tratamiento, análisis e intercambio de información pertinente; b) el apoyo a la formación de personal, así como la cooperación para el intercambio de personal, los equipos y la investigación científica policial; c) las técnicas comunes de investigación relacionadas con la detección de formas graves de delincuencia organizada.[371] En caso de no lograse un acuerdo por medio del procedimiento legislativo ordinario, se establece la posibilidad de una «cooperación reforzada» sobre el proyecto de medidas que se quieran implantar en el ámbito de la cooperación policial. Lo anterior, no es aplicable a los actos que constituyan un desarrollo del Acuerdo Schengen.[372]

Respecto de Europol, el TFUE señala que cumple funciones de apoyo y colaboración con las autoridades policiales y de los demás servicios con funciones coercitivas de los Estados Miembros. Su ámbito de acción se circunscribe, por el momento, a «la prevención de la delincuencia grave que afecte a dos o más Estados Miembros, del terrorismo y de las formas de delincuencia que lesionen un interés

[369] Cfr. COM (2012) 10 final, de 25.1.2012. Al respecto véase *infra*, apartado 2 del capítulo sexto de éste trabajo.
[370] La cooperación policial oficial comenzó en 1976 con la creación de los grupos de Trabajo denominados Grupos Trevi (cooperación basada en la lucha contra el terrorismo, así como en la organización y formación de los servicios policiales). En 1989 los Grupos de Trabajo eran cuatro: terrorismo, cooperación policial, delincuencia organizada y libre circulación de personas. Citado en Joan Lluís PÉREZ FRANCESCH, *La cooperación policial y judicial en el Tratado de Lisboa, entre la europeización y las reservas estatales,* p. 8.
[371] Artículo. 87.2 TFUE.
[372] Artículo 87 párrafo final TFUE. Sobre cooperación policial y el acervo Schengen en el tratado de Lisboa, véase Joan Lluís PÉREZ FRANCESCH, op. cit., p. 8-10.

común que sea objeto de una política de la Unión, así como en la lucha en contra de ellos».[373] Su estructura, funcionamiento, ámbito de actuación y competencias, se regirán por un reglamento adoptado por el procedimiento legislativo ordinario. Es importante consignar que entre sus competencias, expresamente, se mencionan la recogida, almacenamiento, tratamiento, análisis e intercambio de la información, en particular la transmitida por las autoridades de los Estados Miembros o de terceros países o terceras instancias.[374] Por tanto, nos encontramos ante unas de las autoridades europeas habilitadas para realizar tratamientos personales de datos policiales en el ámbito de la cooperación policial en materia penal.[375]

1.5. La protección de datos de carácter personal en el ámbito de la cooperación policial en materia penal

El Tratado de la Unión Europea hacía una referencia expresa a la protección de datos en la cooperación policial.[376] A partir de la entrada en vigencia del Tratado de

[373] Artículo 88.1 TFUE.
[374] Artículo 88.2.a) TFUE.
[375] Sobre la protección de datos en las actividades de Europol, véase *infra*, apartado 4.1 del capítulo sexto de este trabajo. Consúltese también: Patricia ESQUINAS VALVERDE, *Protección de datos personales en la Policía Europea* (Valencia: Tirant lo Blanch, 2010); Viorica-Andreea MARICA, «El sistema de tratamiento de la información en EUROPOL», *Institut de Ciències Polítiques i Socials* WP núm. 309 (2012): pp. 1-33; Anselmo DEL MORAL TORRES, «La cooperación policial en la Unión Europea: propuesta de un modelo europeo de inteligencia criminal», *Análisis del Real Instituto Elcano (ARI)* n.º 50 (2010): pp. 1-12; Alexandra DE MOOR, «The Europol Council Decision: Transforming Europol into an Agency of the European Union - Dialnet», *Common market law review* Vol. 47, Nº 4 (2010): pp. 1089-1121; Raquel CATILLEJO MANZANARES, «Europol y las investigaciones transfronterizas», en *Piratas, mercenarios, soldados, jueces y policías: nuevos desafíos del derecho penal europeo e internacional*, de Luis Alberto Arroyo Zapatero et al. (Cuenca: Universidad de Castilla-La Mancha, 2010); Juan SANTOS VARA, «El desarrollo de la Oficina Europea de Policía (EUROPOL): el control democrático y judicial - Dialnet», en *Los Tratados de Roma en su cincuenta aniversario: perspectivas desde la Asociación Española de Profesores de Derecho Internacional y Relaciones Internacionales* (Madrid: Marcial Pons, 2008): pp. 569-594; Francisco Javier ARROYO ROMERO, *La influencia de Europol en la comunitarización de la policía europea* (Madrid: Akal, 2005); Ricard MARTÍNEZ MARTÍNEZ, «Los datos de carácter personal en el convenio Europol: las comunicaciones de datos a terceros países», en *XIV Encuentros sobre Informática y Derecho: 2000-2001*, de Miguel Ángel DAVARA RODRIGUEZ (Pamplona: Aranzadi, 2001): pp. 129-162; Luis LUENGO ALFONSO, «Cooperación policial y Europol», en *El espacio europeo de libertad, seguridad y justicia*, de Ministerio del Interior (Madrid: Ministerio del Interior. Secretaría General Técnica, 2000): pp. 103-116; SEPD, *Dictamen sobre la propuesta de Decisión del Consejo por la que se crea la Oficina Europea de Policía (Europol)*, COM (2006) 817 final. Diario Oficial n° C 255 de 27/10/2007, pp. 13-21, 27 de octubre de 2007, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006XX1027(02):ES:HTML.
[376] El artículo 30.1.b) disponía: «la acción en común en el ámbito de la cooperación policial incluirá: la recogida, almacenamiento, tratamiento, análisis e intercambio de información pertinente, en particular mediante Europol, incluida la correspondiente a informes sobre operaciones financieras sospechosas que obre en poder de servicios con funciones coercitivas, **con sujeción a las disposiciones correspondientes en materia de protección de datos personales**» [el destacado es nuestro]. Cfr. Versión consolidada del Tratado de la Unión Europea, publicada en el DOCE nº C 325/5, de fecha 24.12.2002.

Lisboa, esta referencia expresa a la protección de datos en la cooperación policial desaparece. El artículo 87 (antiguo artículo 30 TUE) señala que la Unión desarrollará una cooperación policial para la prevención y en la detección e investigación de infracciones penales (artículo 87.1), agregando que el Parlamento Europeo y el Consejo podrán adoptar, con arreglo al procedimiento legislativo ordinario, medidas relativas a la recogida, almacenamiento, tratamiento, análisis e intercambio de información pertinente (artículo 87.2.b); es decir, no se hace referencia al respeto de las normas sobre protección de datos en el caso de tratamientos realizados en el marco de la cooperación policial, lo que a nuestro juicio constituye un retroceso respecto de la normativa anterior a Lisboa.

Actualmente, el derecho a la protección de datos personales se encuentra consagrado en el artículo 16 del TFUE, en los siguientes términos: «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. Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea».[377]

Si bien puede parecer un aspecto puramente formal, creemos que la ubicación sistemática de este artículo: Título II (Disposiciones de aplicación general) de la Primera Parte del TFUE (Principios) demuestra un cambio de criterio y de apreciación de la importancia que se asigna a esta materia actualmente en el espacio europeo. En efecto, la regulación de esta materia pasó de la marginalidad del artículo 286 TCE a los

[377] El nuevo artículo 39 del TUE, situado dentro de la normativa relativa a política exterior y seguridad común (antiguo segundo pilar comunitario) obliga al Consejo a adoptar una decisión que fije las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por los Estados Miembros en el ejercicio de las actividades comprendidas este ámbito de aplicación y sobre la libre circulación de dichos datos. Se señala que el respeto de dichas normas estará sometido al control de autoridades independientes, pero no se especifica si se creará una autoridad especial para tal efecto o se recurrirá a las existentes extendiendo su competencia sobre estas materias.

primeros artículos del TFUE (artículo16). Por otra parte, la competencia legislativa para la regulación sobre esta materia se reparte entre la Unión y los Estados Miembros (artículo 16.2. TFUE). Por último, cabe tener presente la atención sobre la obligación de legislar sobre esta materia que pesa sobre la Unión Europea, sino se estaría incumpliendo el artículo 16 en estudio.

En las declaraciones anejas al Acta Final de la Conferencia intergubernamental que ha adoptado el Tratado de Lisboa, también encontramos referencias a la protección de datos de carácter personal. Así, la declaración relativa al artículo 16 del TFUE señala que siempre que las normas sobre protección de datos de carácter personal que hayan de adoptarse con arreglo a este artículo puedan tener una repercusión directa en la seguridad nacional, habrán de tenerse debidamente en cuenta las características específicas de la cuestión. Recuerda que la legislación actualmente aplicable contiene excepciones específicas a este respecto. En particular, hace un reenvío a las excepciones que se contemplan en la Directiva 95/46/CE.[378] Ésta, al definir su ámbito de aplicación, señala que sus normas no se aplicarán al tratamiento de datos personales que se efectúen en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico de éste cuando dicho tratamiento esté relacionado con su seguridad) y las actividades del Estado en materia penal (artículo 3.2.). Por su parte, el Artículo 13 de la Directiva citada, regula las excepciones y limitaciones de los derechos y obligaciones en materia de protección de datos, permitiendo dichas restricciones, entre otros casos, para la salvaguardia de la seguridad del Estado, la defensa, la seguridad pública, la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas.

En las Declaraciones anejas al Tratado de Lisboa, también encontramos una referencia específica a la protección de datos de carácter personal en el ámbito de la cooperación judicial y policial en materia penal. Esta señala que la Conferencia reconoce

[378] La Directiva 95/46/CE, si bien no se refiere a esta materia bajo la denominación de la seguridad "nacional", hace referencia a la seguridad pública, seguridad del Estado y razones de seguridad de defensa, en los Considerandos 13, 16, 43 y los artículos 3.2.; 13.

que podrían requerirse normas específicas para la protección de éstos y la libre circulación de dichos datos en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial que se basen en el artículo 16 del Tratado de Funcionamiento de la Unión Europea, en razón de la naturaleza específica de dichos ámbitos.[379]

Por último, dentro de las reglas generales y finales del Tratado de Lisboa, el Protocolo (nº 36), dedica su Título VII a las disposiciones transitorias relativas a los actos adoptados en virtud de los títulos V y VI del Tratado de la Unión Europea antes de la entrada en vigor del Tratado de Lisboa. Los efectos jurídicos de los actos de las instituciones, órganos y organismos de la Unión, adoptados en virtud del Tratado de la Unión Europea antes de la entrada en vigor del Tratado de Lisboa, se mantienen en tanto dichos actos no hayan sido derogados, anulados o modificados en aplicación de los Tratados. Lo mismo ocurre con los convenios celebrados entre los Estados miembros sobre la base del Tratado de la Unión Europea (artículo 9 del Protocolo nº 36). En este Protocolo también se señala que las atribuciones de la Comisión en virtud del artículo 258 del TFUE no serán aplicables y las atribuciones del Tribunal de Justicia de la Unión Europea en virtud del título VI del Tratado de la Unión Europea, seguirán siendo las mismas.

En resumen, este Protocolo en sus artículos 9 y 10 dispone que todas las competencias de las instituciones, órganos y organismos de la Unión se mantengan durante cinco años. La Comisión y el Tribunal mantienen su competencia. Si la Comisión modifica algo durante este periodo, pasa a tener competencia el Tribunal. Por tanto, el TJUE, será competente en el ámbito de la cooperación judicial y policial, en relación a los instrumentos legales que se suscriban con posterioridad al Tratado de Lisboa, y respecto de los actos legislativos anteriores al Tratado, no tendrá competencia durante los cinco primeros años de vigencia del Tratado, salvo que sean modificados.[380]

[379] Cfr. Declaración Nº 21, aneja al Acta Final de la Conferencia intergubernamental que ha adoptado el Tratado de Lisboa firmado el 13 de diciembre de 2007, relativa a la protección de datos de carácter personal en el ámbito de la cooperación judicial en materia penal y de la cooperación policial.
[380] Artículo 10 del Protocolo 10).

2. CARTA DE DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA

2.1. CDFUE como fuente del derecho europeo

Los Tratados constitutivos de la Comunidad Europea no incluyeron un catálogo de derechos ni disposiciones específicas sobre derechos fundamentales.[381] Dicha ausencia se explica por la naturaleza esencialmente económica de los mismos, sumada a que «la ideología de los derechos todavía no había alcanzado la importancia y el ascendiente que después ha tenido».[382] De esta forma, por lo que en materia de derechos fundamentales se refiere, el Convenio Europeo de Derecho Humanos del Consejo de Europa constituía el único instrumento normativo de garantía en la materia.[383]

No obstante la ausencia de un catálogo de derechos fundamentales en los tratados constitutivos de la Comunidad Europea, el Tribunal de Justicia de las Comunidades Europeas (en adelante, TJCE), como ente encargado de la interpretación y aplicación de los Tratados[384], elaboró una doctrina de acuerdo con la cual los derechos fundamentales formaban parte del ordenamiento comunitario como principios generales del derecho.[385] Esta doctrina se incorporó formalmente al derecho originario por medio

[381] Cfr. Tratado de la Comunidad Europea del Carbón y del Acero (CECA) de 1951; Tratado de Roma o Tratado constitutivo de la Comunidad Económica y Europea (TCEE) por el que se instituyó la Comunidad Económica Europea, y el Tratado constitutivo de la Comunidad Europea de la Energía Atómica (EURATOM) en 1957 y el Acta Única Europea de 1965.

[382] Francisco RUBIO LLORENTE, «Los derechos fundamentales en la Unión Europea y el estatuto de la Carta», *EuropaFutura.org* nº 4 (mayo de 2004), p. 17. En la misma línea, véase Mónica ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa* (Valencia: Tirant lo Blanch, 2006). pp. 191-194; Montserrat PI LLORENS, *Los derechos fundamentales en el ordenamiento comunitario* (Barcelona: Ariel, 1999), pp. 19-22.

[383] Sobre el CEDH véase *supra*, apartado 1 del capítulo cuarto de este trabajo.

[384] El artículo 220 TCE disponía que: «El Tribunal de Justicia y el Tribunal de Primera Instancia garantizarán, en el marco de sus respectivas competencias, el respeto del Derecho en la interpretación y aplicación del presente Tratado…».

[385] Sobre el proceso de evolución de la doctrina del TJCE, Mónica Arenas señala que «…entre finales de los años cincuenta y principios de los sesenta del siglo XX, con motivo de la resolución de diversas demandas, el TJCE se planteó la cuestión de la protección eficaz de los derechos fundamentales en el ordenamiento comunitario. En esas demandas se solicitaba la anulación de determinadas disposiciones comunitarias por entender que lesionaban derechos fundamentales consagrados en las Constituciones de los Estados Miembros. El Tribunal, rechazó pronunciarse sobre el tema alegando ser incompetente para interpretar y aplicar normas nacionales, de acuerdo con las competencias que tenía atribuidas. Y por ello, debido a la negativa del TJCE a pronunciarse sobre las cuestiones relativas a derechos fundamentales que se le planteaban, a esta etapa se la ha denominado "inhibicionista". Por su parte, los Tribunales Constitucionales, en especial el alemán y el italiano, afirmaron que si el TJCE no tenía competencia para pronunciarse sobre derechos fundamentales reconocidos en sus respectivas Constituciones, debían ser ellos mismos los que se pronunciasen en esos casos. Esto se ha conocido como la "rebelión de los Tribunales constitucionales". Sin embargo, posteriormente, el TJCE reaccionaría y comenzaría a

del Tratado de la Unión Europea (en adelante, TUE) de 1992.[386] El artículo 6.2 del TUE disponía que «La Unión respetará los derechos fundamentales tal y como se garantizan en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, firmado en Roma el 4 de noviembre de 1950, tal y como resultan de las tradiciones constitucionales comunes a los Estados Miembros como principios generales del Derecho Comunitario». Con ello, se conectaba tres sistemas jurídicos diferentes: el de la Unión Europea, el del Consejo de Europa y el de los Estados Miembros, de manera que para determinar cuáles son los derechos fundamentales comunitarios, se debía recurrir al CEDH y los derechos reconocidos por el TJCE como tradiciones constitucionales comunes.[387] Ahora bien, este sistema de reconocimiento y garantía de los derechos fundamentales en la Unión Europea, establecido por los artículos 6 y 46 del TUE, no suplía la ausencia de un catálogo propio de derechos fundamentales. Por tanto, era el TJCE el que decidía, en cada caso concreto, si un derecho fundamental debía o no ser considerado como parte integrante del derecho comunitario, lo que provocaba una falta de seguridad jurídica sobre el tema.[388] Como forma de superar esta falta de seguridad jurídica, la opción política contemplada por las instituciones comunitarias se centró en una posible adhesión de la Comunidad Europea al CEDH[389], pero esto era imposible sin una revisión del Tratado.

---

reconocer de un modo gradual su competencia sobre la protección de los derechos fundamentales en el ordenamiento comunitario». Cfr. ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, 193-194, y la bibliografía y jurisprudencia citada por la autora.

[386] El Tratado de la Unión Europea, conocido también como Tratado de Maastricht por haber sido firmado el 7 de febrero de 1992 en la localidad holandesa homónima, es un Tratado que modifica los Tratados fundacionales de las Comunidades Europeas (Tratado de París (1951), los Tratados de Roma de 1957 y el Acta Única Europea de 1986). Constituye un paso crucial en el proceso de integración europeo, pues se sobrepasaba por primera vez el objetivo económico inicial de las Comunidades y se le da una vocación de carácter político. Con este Tratado se crea la Unión Europea, que engloba en sí las tres Comunidades Europeas anteriores, aunque con modificaciones sustanciales sobre todo de la Comunidad Económica Europea, que pasa a llamarse Comunidad Europea. Además, se adoptan dos sistemas de cooperación intergubernamental: la Política Exterior y de Seguridad Común (PESC) y la Cooperación en Asuntos de Interior y de Justicia (CAJI).

[387] Al respecto véase Teresa FREIXES SANJUÁN y Juan Carlos REMOTTI CARBONEL, *El futuro de Europa. Constitución y derechos fundamentales,* (Valencia: Mimin Ediciones, 2002), p. 92-94.

[388] Arenas Ramiro, *El derecho fundamental a la protección de datos personales en Europa*, p. 202.

[389] Cfr. los Memorándum de la Comisión de 4 de abril de 1979, reiterados el 19 de noviembre de 1990 y el 26 de octubre de 1993 con el documento «La adhesión de la Comunidad al Convenio Europeo de Derechos humanos y el ordenamiento jurídico comunitario»; y las Resoluciones del Parlamento de 18 de enero de 1994 y de 16 de marzo de 2000. Al respecto, véase CHUECA SANCHO, "Por una Europa de los derechos humanos: la adhesión de la Unión Europea al Convenio Europeo de Derechos Humanos".; M. Paloma BIGLINO CAMPOS, "De qué hablamos en Europa cuando hablamos de Derechos fundamentales: el argumento de Hamilton", *Revista de Derecho Comunitario Europeo* nº 14 (2003): p. 99.; Teresa FREIXAS SANJUÁN, «Las principales construcciones jurisprudenciales del Tribunal Europeo de Derechos Humanos», en *Los derechos en Europa*, ed. Yolanda Gómez Sánchez (Madrid: Universidad Nacional de Educación a Distancia, UNED, 1997): p. 99; Peter HÄBERLE, «Derecho

Por ello se opta por la elaboración de una Carta de Derechos Fundamentales de la Unión (en adelante, la Carta o CDFUE).[390] Con la codificación que realiza la Carta, los derechos salen de la penumbra, se visibilizan, lo que permite que los ciudadanos tengan certeza respecto de cuáles son sus derechos.[391]

La Convención que elaboró la Carta se compuso de representantes de todas las instancias ejecutivas y legislativas de la Unión y de los Estados Miembros, sin que existiera ningún tipo de jerarquía entre ellos.[392] El hecho de que la elaboración de la Carta se encargara a la Convención, utilizando un método intermedio entre el parlamentario y el intergubernamental, hizo que fuera un procedimiento especialmente transparente y participativo, lo cual, le confería un plus de legitimidad una vez aprobada.[393] El Trabajo de la Convención, termina con la proclamación solemne de la

---

constitucional común europeo», en *Derechos humanos y constitucionalismo ante el tercer milenio* (Madrid: Marcial Pons, 1996): pp. 187-224.

[390] Sobre la Carta de Derecho Fundamental de la Unión Europea existe una abundante bibliografía, entre otros véase Juan Antonio CARRILLO SALCEDO, «Notas sobre el significado político y jurídico de la Carta de los Derechos Fundamentales de la Unión Europea», *Revista de Derecho Comunitario Europeo* nº 9 (2001): pp. 7-26; A. FERNÁNDEZ TOMÁS, «Sobre la eficacia de la Carta de Derechos Fundamentales de la Unión Europea», en *La Carta de Derechos Fundamentales de la Unión Europea* (Zamora: Cuadernos del Instituto Rei Alfonso Henriques de Cooperación Transfronteriza, 2003): pp. 33-48; Alberto HERRERO DE LA FUENTE, ed., *La Carta de Derechos Fundamentales de la Unión Europea: una perspectiva pluridisciplinar* (Valencia: Tirant Lo Blanch, 2003); Juan Francisco MORENO DOMÍNGUEZ, «La Carta de los Derechos Fundamentales de la Unión Europea: desde la solemnidad a la eficacia», Artículo, 5 de febrero de 2010, http://rabida.uhu.es/dspace/handle/10272/2547; RUBIO LLORENTE, «Los derechos fundamentales en la Unión Europea y el estatuto de la Carta»; Carlos RUÍZ MIGUEL, «El largo y tortuoso camino hacia la Carta de los Derechos Fundamentales de la Unión Europea», *Revista europea de derechos fundamentales* n.º 2 (2003): pp. 61-90. Teresa PAREJO NAVAJAS, «La Carta de los derechos fundamentales de la Unión Europea», *Derechos y Libertades: Revista de filosofía del derecho y derechos humanos*, enero de 2010: pp. 205-239.

[391] Al respecto se ha señalado que «los derechos fundamentales sólo pueden cumplir su función si los ciudadanos conocen su existencia y son conscientes de la posibilidad de hacerlos aplicar, por lo que resulta esencial expresar y presentar los derechos fundamentales de forma que todos los individuos puedan conocerlos y tener acceso a ellos; dicho de otro modo, los derechos fundamentales deben ser "visibles"». Cfr. El Informe SIMITIS de febrero de 1999. En la misma línea, Mónica ARENAS RAMIRO, plantea que la visibilización de los derechos es el principal aporte de la Carta. Cfr. *El derecho fundamental…,* op. cit., p. 203.

[392] Su composición y método de trabajo quedó fijado en el Consejo Europeo de Tampere, de octubre de 1999. Se optó por una composición cuadripartita, con 62 miembros, representantes de Jefes de Estado y de Gobierno, del Parlamento Europeo, de los Parlamentos nacionales y del Presidente de la Comisión Europea, además de 4 observadores permanentes de TJCE, del TEDH y del Consejo de Europa. Sobre las justificaciones políticas e históricas de la Carta, así como de las críticas en cuanto a su denominación, FERNÁNDEZ TOMÁS, «Sobre la eficacia de la Carta de Derechos Fundamentales de la Unión Europea»; Juan Antonio CARRILLO SALCEDO, «Notas sobre el significado político y jurídico de la Carta de los Derechos Fundamentales de la Unión Europea», *Revista de Derecho Comunitario Europeo* nº 9 (2001): p. 9; Pablo RUIZ-JARABO, «La Carta de Derechos Fundamentales de la Unión europea y su renuncia a regular la competencia de los tribunales Comunitarios y de Derechos Humanos: ¿Virtud o defecto?», *Noticias de la Unión Europea* nº 207 (2002): p. 9.

[393] Al respecto, Mónica ARENAS, señala que «Este método suponía un avance considerable en la medida en que, como se ha dicho, se pretendía llevar a cabo el proceso de construcción europea desde abajo hacia arriba y no al contrario como se venía haciendo hasta ahora.» Cfr. ARENAS RAMIRO, *El derecho*

Carta de los Derechos Fundamentales de la Unión Europea por el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea el 7 de diciembre de 2000 en el Consejo Europeo de Niza.[394] Además de la Carta propiamente dicha, redactaron también unas «explicaciones» que detallan el origen de cada precepto y sirven como guía en la interpretación de la misma.[395]

La Carta de los Derechos Fundamentales de la Unión Europea se estructura en dos partes: un preámbulo introductorio y siete títulos que recogen los cincuenta y cuatro artículos la integran. Cada título trata sobre un derecho, destinando el último de éstos a las disposiciones generales que rigen la interpretación y aplicación de la Carta. De esta forma se rompe con la estructura clásica que distingue entre derechos civiles y políticos, y los derechos económicos y sociales, evitando de esta forma introducir cualquier tipo de jerarquía entre los derechos.[396]

En cuanto al contenido de la CDFUE, si bien se inspira ampliamente en los derechos establecidos en otros instrumentos como el CEDH, la Carta Social Europea o la Carta Comunitaria de los Derechos Sociales, así como también en la jurisprudencia del TEDH y el TJCE, y las Constituciones de los Estados Miembros, ello no implica

---

fundamental a la protección de datos personales en Europa, 205 y 206. En el mismo sentido, véase Francisco RUBIO LLORENTE, «Mostrar los derechos sin destruir la Unión», en *La encrucijada constitucional de la Unión Europea: Seminario internacional organizado por el Colegio Libre de Eméritos en la real Academia de Ciencias Morales y Políticas, en Madrid, los días 6, 7 y 8 de noviembre de 2001* (Madrid: Civitas, 2002), p. 32.; Juan Antonio CARRILLO SALCEDO, «Notas sobre el significado político y jurídico de la Carta de los Derechos Fundamentales de la Unión Europea», pp. 8-9.

[394] La Convención aprobó el proyecto definitivo el 21.7.2000 y lo concluyó el 2.10.2000, presentando el texto definitivo de la Carta en el Consejo informal de Biarritz el 14 de octubre y proclamándose solemnemente en el Consejo de Niza de 7.12.2000. Publicado en el DOUE n° C 364, de 18.12.2000. Al respecto véase Para un estudio detallado sobre la CDFUE, véase Juan Antonio CARRILLO SALCEDO, «Notas sobre el significado político y jurídico de la Carta de los Derechos Fundamentales de la Unión Europea». *Revista de Derecho Comunitario Europeo* nº 9 (2001): pp. 7-26; Alberto HERRERO DE LA FUENTE, ed. *La Carta de Derechos Fundamentales de la Unión Europea: una perspectiva pluridisciplinar*. Valencia: Tirant Lo Blanch, 2003; Juan Francisco MORENO DOMÍNGUEZ, «La carta de los derechos fundamentales de la Unión Europea: desde la solemnidad a la eficacia». Artículo, 5 de febrero de 2010. *http://rabida.uhu.es/dspace/handle/10272/2547*; Teresa PAREJO NAVAJAS, «La Carta de los derechos fundamentales de la Unión Europea». *Derechos y Libertades: Revista de filosofía del derecho y derechos humanos*, enero de 2010; Francisco RUBIO LLORENTE, «Los derechos fundamentales en la Unión Europea y el estatuto de la Carta». *EuropaFutura.org*, nº 4 (mayo de 2004): pp. 15-27; Carlos RUIZ MIGUEL, «El largo y tortuoso camino hacia la Carta de los Derechos Fundamentales de la Unión Europea». *Revista europea de derechos fundamentales*, nº 2 (2003): pp. 61-90.

[395] Cfr. Explicaciones sobre la Carta de los Derechos Fundamentales, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0017:0035:ES:PDF [Consultado el 23.7.2013]

[396] Sobre la estructura de la Carta, véase Mónica ARENAS…, op. cit., p. 207 y la bibliografía citada por la autora.

que sea un texto meramente compilatorio, ya que incorporan las novedades correspondientes en las distintas materias.[397] Así, la Carta, junto con recoger los denominados «derechos clásicos», incorpora nuevos derechos o «derechos de nueva generación», los cuales provienen de evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos, entre los cuales podríamos situar a la protección de datos personales. Por otra parte, el hecho que la Carta recoja nuevos derechos, ha servido en el proceso de armonización las normas nacionales de los Estados Miembros.[398] En relación al contenido de la Carta, también es interesante la distinción que realiza la misma entre «derechos», «libertades» y «principios». Desde el punto de vista normativo los derechos limitarían el poder de las instituciones y órganos de la Unión, e incluso el de los Estados al aplicar el derecho comunitario, al reconocer a su titular una determinada posición jurídica subjetiva de poder, es decir, un haz de facultades que ejerce frente a dichos poderes públicos. Por el contrario, los principios, imponen a sus destinatarios la obligación de observarlos y promover su aplicación con arreglo a sus respectivas competencias.[399]

La Carta se aplica, en primer lugar, a las instituciones, órganos y organismos de la Unión (artículo 51, apartado 1, de la Carta). Por consiguiente, rige, en particular, el trabajo legislativo y decisorio de la Comisión, del Parlamento y del Consejo, cuyos actos jurídicos deben ajustarse plenamente a la Carta. En cuanto a los Estados Miembros, la misma disposición establece que solo se aplica cuando ponen en práctica el Derecho de la Unión. No se aplica, por tanto, en las situaciones que no tengan

[397] El Preámbulo de la Carta de los Derechos Fundamentales de la Unión Europea, señala que los derechos y principios recogidos en la Carta se derivan, en particular, de las tradiciones constitucionales y de las obligaciones (Convenios) internacionales comunes de Estados Miembros, del Convenio Europeo de Derechos Humanos, de las Cartas sociales adoptadas por la Comunidad y por el Consejo de Europa, así como de la Jurisprudencia del Tribunal de Justicia de la Unión y del Tribunal Europeo de Derechos Humanos. Al respecto véase, ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, pp. 208-211 y bibliografía citada por la autora.

[398] Ibídem, p. 211.

[399] El artículo 51 de la Carta establece expresamente que «...éstos [instituciones, órganos y organismos de la Unión] respetarán los derechos, observarán los principios y promoverán su aplicación...». Esta distinción entre derechos, libertades y principios es más claro en el apartado 1 del artículo 6 del TUE, que dispone que «La Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea […] la cual tendrá el mismo valor jurídico que los Tratados». Al respecto véase, Francisco RUBIO LLORENTE, "Mostrar los derechos...", op. cit., pp. 134-138; y del mismo autor, "Una Carta de...", op. cit., pp. 191-193; y "Los derechos fundamentales...", op. cit., pp. 22- 23; Álvaro RODRÍGUEZ BEREIJO, "La Carta de.. ", op. cit., pp. 33-34, para quien esta distinción no provocaba ningún tipo de jerarquía; y Pedro CRUZ VILLALÓN, "La Carta de Derecho y la Constitución española", en *Revista parlamentaria de la Asamblea de Madrid*, nº 12, 2005, pp. 10 y 15-18; y Mónica ARENAS RAMIRO, *El derecho fundamental…,* op. cit., p. 208.

ninguna relación con ésta.[400] La fuerza jurídica vinculante conferida a la Carta por el Tratado de Lisboa no ha modificado esta situación, ya que este último especifica claramente que las disposiciones de la Carta no amplían, en modo alguno, las competencias de la Unión tal como quedan definidas en los Tratados.[401]

2.2. El derecho a la protección de datos como derecho fundamental autónomo

La Carta de Derecho Fundamentales de la Unión Europea, proclamada en Niza el año 2000, recoge en su catálogo de derechos fundamentales el derecho a la protección de datos personales. A diferencia del CEDH, en que sólo se reconoce el derecho a la vida privada,[402] la Carta de Derechos Fundamentales de la Unión Europea, va a reconocer por una parte, el derecho al respeto a la vida privada y familiar (artículo 7), y por otro, el derecho a la protección de datos personales (artículo 8), es decir, consagra ambos derechos de forma independiente y autónoma.

El artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, bajo el título «Protección de datos de carácter personal», establece que: «1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente».

[400] Al respecto véase el punto 1.3 de la «Estrategia para la aplicación efectiva de la Carta de los Derechos Fundamentales por la Unión Europea», op. cit., pp. 10 y ss.

[401] El artículo 51, apartado 2, de la Carta, dispone que no amplía el ámbito de aplicación del Derecho de la Unión más allá de las competencias de la Unión, ni crea ninguna competencia o misión nuevas para la Unión, ni modifica las competencias y misiones definidas en los Tratados.

[402] Lo anterior es de toda lógica, toda vez que dicho instrumento fue elaborado terminada la segunda guerra mundial y suscrita en 1950, es decir, cuando la informática daba sus primeros pasos y la afectación de los derechos por parte de la misma sólo constituía una amenaza más eventual que real. De todas formas, el proceso de reconocimiento de la protección de datos personales como un derecho vino de la mano de la labor interpretativa que realizó el TEDH, que llegó a establecer, a partir del derecho a la vida privada reconocido en el art. 8 del CEDH, una dimensión informacional de la misma, devenida posteriormente en el derecho a la protección de datos personales. Al respecto véase Mónica ARENAS RAMIRO, *El derecho fundamental…*, op. cit. pp. 225-248; Abel TELLEZ AGUILERA, *La protección de datos en la Unión Europea* (Madrid: Edisofer, 2002), pp. 59-65.

Para la elaboración del artículo 8 del CDFUE, se tuvieron como bases tanto el artículo 286 del Tratado constitutivo de la Comunidad Europea[403] y en la Directiva 95/46/CE[404] del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, así como en el artículo 8 del CEDH y en el Convenio nº 108, ambos del Consejo de Europa. También, y aunque no se señale expresamente, se tuvieron en consideración como fuentes de inspiración al momento de redactar este artículo 8 de la Carta, las tradiciones constitucionales comunes de los Estados Miembros, así como los artículo 18 de la Declaración del Parlamento Europeo sobre derechos fundamentales y libertades públicas, de 12 de abril de 1989, y el artículo 17 del Pacto Internacional de derechos civiles y políticos.[405]

El reconocimiento de este derecho, como un derecho autónomo del derecho a vida privada, se debe a la toma de conciencia de que es necesario garantizar una tutela específica y efectiva frente a la recogida y almacenamiento de información sobre las personas, dado su carácter potencialmente peligroso para algunos derechos fundamentales, y en especial, para la privacidad y los datos personles. Es fácil comprobar cómo los avances tecnológicos permiten utilizar medios electrónicos o automatizados en la gestión de la información, que han facilitado la posibilidad de crear bancos de datos y de hacer circular la información contenida en ellos. Es más, la propia integración europea ha traído consigo la intensificación del flujo transfronterizo de datos, lo que ha hecho más patente aún para las instituciones comunitarias la necesidad

[403] Artículo 286: 1. A partir del 1 de enero de 1999, los actos comunitarios relativos a la protección de las personas respecto del tratamiento de datos personales y a la libre circulación de dichos datos serán de aplicación a las instituciones y organismos establecidos por el presente Tratado o sobre la base del mismo. 2. Con anterioridad a la fecha indicada en el apartado 1, el Consejo establecerá, con arreglo al procedimiento previsto en el artículo 251, un organismo de vigilancia independiente, responsable de controlar la aplicación de dichos actos comunitarios a las instituciones y organismos de la Comunidad y adoptará, en su caso, cualesquiera otras disposiciones pertinentes.

[404] Publicada en el DOCE n° L 281, de 23 de noviembre de 1995. Respecto de esta Directiva, véase el apartado siguiente.

[405] Algunos autores agregan como factor subjetivo en la consagración del derecho a la protección de datos personales como un derecho fundamental distinto y autónomo de la vida privada, que el Presidente de la Convención que elaboró la Carta era el constitucionalista alemán Roman Herzog, quien fuera miembro del Tribunal Constitucional Federal Alemán, durante el periodo en el que se configuró el derecho a la autodeterminación informativa. Cfr. Carlos RUIZ MIGUEL, «El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea», en *La Carta de Derechos Fundamentales de la Unión Europea: una perspectiva pluridisciplinar* (Valencia: Fundación Rei Afonso Henriques - Tirant Lo Blanch, 2003), pp. 173-210.

de establecer un estándar mínimo de principios, derechos, obligaciones y garantía en materia de protección de los datos personales.[406]

El artículo 8 de la Carta no define expresamente qué se debe entender por «datos personales» ni de «tratamiento de datos personales», pero en los trabajos preparatorios y la explicaciones de la misma, hacen una remisión a la legislación comunitaria y del Consejo de Europa sobre la materia. Por tanto, debemos entender que los conceptos señalados se refieren a «toda información relativa a una persona identificada o identificable» y «toda aquella actividad realizada con datos personales, independientemente de si se realiza de forma automatizada o manual, pero siempre que los datos estén o vayan a estar en ficheros», respectivamente.[407] Estas definiciones son tecnológicamente neutras, lo que posibilita integrar a su contenido cualquier nueva forma de tratamiento de datos personales que vaya apareciendo.[408]

En cuanto al ejercicio del derecho a la protección de los datos de carácter personal, el documento explicativo de la CDFUE señala que se ejercerá en las condiciones establecidas por la Directiva 95/46/CE y puede limitarse en las condiciones establecidas por el artículo 52 de la Carta. Éste último artículo, que regula el alcance de los derechos garantizados, señala que cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Sólo se podrán introducir limitaciones, respetando el principio de proporcionalidad, 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. El derecho a la protección de datos personales, al igual que los otros derechos reconocidos por la CDFUE, tienen su fundamento en los tratados comunitarios o en el Tratado de la Unión Europea y se ejercen en las condiciones y dentro de los límites determinados por éstos.[409] Como ya hemos señalado, en la medida en que la Carta de Derechos Fundamentales de la Unión Europea contenga derechos que correspondan a derechos

[406] El mismo sentido véase Mónica ARENAS, op. cit., p. 245.
[407] Cfr. artículo 2.a) y b) de la Directiva 95/46/CE. En las últimas normas de la Unión Europea podemos ver un cambio en la definición de que se debe entender por «dato personal», así por ejemplo, la nueva Propuesta de Directiva en el ámbito de la prevención y represión penal, , lo define en términos más sencillos, como «toda información relativa a un interesado». Cfr. COM (2012) 10 final, p. 28.
[408] En el mismo sentido Mónica ARENAS, op. cit., p. 243.
[409] Artículo 52.1 CDFUE.

garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, su sentido y alcance serán iguales a los que les confiere dicho Convenio. No obstante, ello no impide que el Derecho de la Unión conceda una protección más extensa.[410]

El derecho a la protección de datos personales consagrado en el artículo 8 de la Carta está íntimamente vinculado con otros derechos fundamentales reconocidos en la misma Carta. De partida, el artículo 8 tiene como sustrato, al igual que todos los derechos fundamentales consagrados, el respeto a la dignidad humana.[411] Asimismo, el derecho reconocido en el artículo 8 de la CDFUE tiene una conexión evidente con el derecho a la vida privada, reconocido en el artículo 7 de la misma Carta.[412] Es más, durante la elaboración de la Carta, se planteó la posibilidad de que el derecho a la vida privada incluyera dentro de su ámbito de protección a la autodeterminación informativa.[413] Otros derechos fundamentales consagrados en la Carta, que tienen una directa relación con la protección de los datos personales son: la prohibición de cualquier tipo de discriminación, y en particular la ejercida por razón de raza, orígenes étnicos, características genéticas, religión o convicciones, opiniones políticas o de cualquier otro tipo, discapacidad u orientación sexual[414]; los derechos del menor[415]; y el derecho a la tutela judicial efectiva y a un juez imparcial.[416]

---

[410] Artículo 52.3 CDFUE.

[411] Artículo 1 CDFUE.

[412] Artículo 7: «Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones». En el texto explicativo de la Carta de Derechos Fundamentales de la Unión Europea, se señala que los derechos garantizados en el artículo 7 corresponden a los que garantiza el artículo 8 del Convenio Europeo de Derechos Humanos y de conformidad con lo dispuesto en el apartado 3 del artículo 52 de la CDFUE, este derecho tiene el mismo sentido y alcance que el artículo 8 del CEDH. Por tanto, en la medida en que la presente Carta contenga derechos que correspondan a derechos garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, su sentido y alcance serán iguales a los que les confiere dicho Convenio (artículo 52.3 CDFUE). Como consecuencia de anterior, las limitaciones de que puede ser objeto legítimamente este derecho son las mismas que las toleradas en el marco del referido artículo 8 del CEDH. Esto es, que las injerencias esté previstas por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás (artículo 8.2. CEDH).

[413] Al respecto véase Mónica ARENAS, op. cit., p. 244-245.

[414] Artículo 21 CDFUE.

[415] Artículo 24 CDFUE.

[416] Artículo 47 CDFUE. Estas relaciones y remisiones entre derechos fundamentales consagrados en la Carta, se mencionan también en las nuevas propuestas legislativas de la Unión, v.g. la Propuesta de Directiva, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos, COM(2012) 10 final, de 25.1.2012, pp. 6 y 7.

Para que la Carta surta todos sus efectos en la actual era digital, la Comisión ha propuesto una serie de importantes reformas a las normas de la UE en materia de protección de los datos personales.[417] Las propuestas de reforma buscan actualizar y modernizar los principios consagrados en la Directiva de 1995 para garantizar el derecho a la protección de los datos personales en el futuro, incrementando la responsabilidad y la obligación de rendir cuentas de todos aquellos que procesan los datos personales; reforzando el papel de las autoridades nacionales independientes con competencias en la materia; e introduciendo el «derecho al olvido», que ayudará a los ciudadanos a gestionar mejor los riesgos que afectan a la protección de los datos en línea.[418] En el ámbito específico del antiguo tercer pilar comunitario, las reformas buscan ampliar los principios y normas generales en materia de protección de datos a las administraciones nacionales de policía y justicia penal, superado de esta forma una de las principales críticas que se le planteaban a la Decisión Marco 2008/977/JAI que regula, precisamente, la protección de datos personales en el ámbito de la cooperación policial y judicial en materia penal.

2.3. Reconocimiento de la CDFUE en el Tratado de Lisboa y su impacto para el derecho fundamental a la protección de datos

En un principio, el Parlamento Europeo autorizó a la Presidencia de la Convención únicamente a «proclamar» el texto de la Carta, pero se dejó en suspenso el alcance que tendría la misma.[419] Ello da cuenta de las diferentes posiciones que existían entre los miembros de la Convención, donde algunos abogaban por su integración a los Tratados originarios, y otros, se mostraban abiertamente contrarios a reconocer eficacia

[417] Al respecto, véase «la protección de la privacidad en un mundo interconectado – Un Marco Europeo de Protección de Datos para el siglo XXI», COM (2012) 09 final; la «Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos», COM (2012) 11final; y la «Propuesta de Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos», COM (2012) 10 final. Los dos últimos documentos mencionados son analizados en profundidad en los siguientes apartados de esta tesis.

[418] Informe de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 8 de mayo de 2013, «Informe de 2012 sobre la aplicación de la Carta de los Derechos Fundamentales de la UE. COM (2013) 271 final», p. 3.

[419] Cfr. Recomendación del Parlamento Europeo, de 14 de noviembre de 2000.

jurídica directa y vinculante a la Carta.[420] De esta forma, mientras la CDFUE no tuviera un reconocimiento expreso como norma jurídica vinculante, los Tribunales tanto nacionales como el TJCE sólo podían utilizar la Carta como fuente de interpretación, pero no aplicarla directamente.[421]

La situación anteriormente descrita cambia el 12 de diciembre de 2007, cuando los Presidentes del Parlamento, del Consejo y de la Comisión Europea firmaron y volvieron a proclamar solemnemente la Carta.[422] Esta segunda proclamación era necesaria porque la Carta que se proclamó en 2000 fue adaptada para que fuera jurídicamente vinculante en el Tratado de Lisboa. Si bien la CDFUE no forma parte del texto del Tratado de Lisboa, por remisión del actual artículo 6 del Tratado de la Unión Europea, se hace vinculante para todos los Estados con el mismo valor jurídico que los Tratados (TUE y TFUE). De esta forma, los derechos, libertades y principios enunciados en la Carta pasan a ser legalmente vinculante para todos los países de la Unión que ratificaron el Tratado de Lisboa, lo que le confiere una mayor visibilidad y seguridad jurídica para los ciudadanos.

---

[420] Entre los países miembros de la Convención que eran abiertamente contrarios a otorgarle carácter jurídico vinculante a la Carta, encontramos a los suecos, daneses, finlandeses, irlandeses y británicos; otros más bien reticentes, como holandeses, austriacos, franceses, alemanes y portugueses. Por último, entre los partidarios de su integración en los Tratados, encontramos al Parlamento Europeo, la Comisión, el Comité Económico y Social, el Comité de las Regiones e incluso la propia Convención, así como los italianos, los españoles, los belgas, los luxemburgueses y los griegos. Cfr. Comunicación de la Comisión, de 11 de octubre de 2000, sobre la naturaleza de la Carta, COM (2000) 644 final; Resoluciones Parlamento, de 16 de marzo, 2 de octubre y de 14 de diciembre de 2000; Comunicación de la Comisión, de 28 de septiembre de 2000; Dictamen del Comité Económico y Social, de 20 de septiembre de 2000; Resolución del Comité de la Regiones, de 20 de septiembre y 13 de diciembre de 2000. Al respecto, véase Mónica ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, pp. 212-213; Ricardo ALONSO GARCÍA, «Las cláusulas horizontales de la Carta de Derechos Fundamentales de la Unión Europea», en *la encrucijada constitucional de la Unión Europea*, ed. Eduardo GARCÍA de ENTERRÍA (Madrid: Civitas, 2002), p. 210, http://pendientedemigracion.ucm.es/info/kinesis/ceuropa.htm; CARRILLO SALCEDO, «Notas sobre el significado político y jurídico de la Carta de los Derechos Fundamentales de la Unión Europea», p. 20; Álvaro RODRÍGUEZ BEREIJO y Eduardo GARCÍA de ENTERRÍA, «El valor jurídico de la Carta de los Derechos Fundamentales de la Unión Europea después del Tratado de Niza», en *La encrucijada constitucional de la Unión Europea* (Madrid: Civitas, 2002), p. 210, http://pendientedemigracion.ucm.es/info/kinesis/ceuropa.htm; Alessandro PACE, «¿Para qué sirve la Carta de Derechos Fundamentales de la Unión Europea?», *Teoría y Realidad Constitucional* N° 7 (2001): p. 174.

[421] Así, la Carta pasó a formar parte de lo que se denomina *«soft law»*, es decir, aquellas normas que permiten interpretar o completar disposiciones comunitarias que sí están dotadas de fuerza jurídica vinculante. El TJCE se ha pronunciado sobre la eficacia de las normas de *soft law* y ha estimado que los tribunales nacionales están obligados a tener en cuenta este tipo de normas en la medida en que sean susceptibles de iluminar la interpretación de aquellas otras disposiciones, de efecto obligatorio, que los órganos nacionales deban aplicar, o cuando tengan por objeto completar disposiciones comunitarias que sí estén dotadas de fuerza vinculante. Al respecto véase ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, pp. 214-218 y la jurisprudencia citada por la autora.

[422] http://europa.eu/rapid/press-release_IP-07-1916_es.htm [consulta: 05.10.2013]

Después de la entrada en vigor del Tratado de Lisboa, la Comisión se ha planteado como objetivo político concentrar sus esfuerzos en la aplicación efectiva de los derechos consagrados en la CDFUE. Para ello ha elaborado una estrategia que busca, precisamente, hacer que los derechos fundamentales recogidos en la Carta sean lo más efectivos posible en la Unión.[423] Con ello se busca que la Unión Europea sea un "ejemplo" de respeto de los derechos fundamentales, «lo que permite fomentar la confianza entre los Estados Miembros, así como la del público en general respecto a las políticas de la Unión».[424]

La aplicación sistemática de la Carta exige no sólo un control «jurídico» riguroso, sino también un control «político» para determinar las repercusiones de todas las iniciativas de la UE sobre los derechos fundamentales. En esta línea, la Comisión estableció como una de las estrategias que buscan la aplicación efectiva de los derechos consagrados en la CDFUE, la realización de un informe anual sobre las medidas concretas adoptadas para la aplicación efectiva de la Carta.[425]

Por último, el paso de la Carta de los Derechos Fundamentales de la Unión Europea de un instrumento meramente declarativo e interpretación —*soft law*— a Derecho vinculante para las Instituciones europeas, los Estados Miembros y sus ciudadanos —*hard o proper law*— a través de su inclusión en el Tratado de Lisboa, suscita muchos temas de interés. Uno de ellos, es la referida a la forma cómo se articularan los mecanismos de protección de los derechos fundamentales como consecuencia de la coexistencia de diversos sistemas jurídicos reguladores de tales

[423] Cfr. Comunicación de la Comisión de 19.10.2010, «Estrategia para la aplicación efectiva de la Carta de los
Derechos Fundamentales por la Unión Europea», COM(2010) 573 final;
[424] Al respecto, la Comisión ha señalado que « La actuación de la Unión debe ser irreprochable en materia de derechos fundamentales. La Carta debe ser una guía para las políticas de la Unión y para su aplicación por los Estados Miembros». Cfr. la «Estrategia para la aplicación efectiva de la Carta de los Derechos Fundamentales por la Unión Europea», p. 4.
[425] Sobre la aplicación de la Carta y los problemas concretos a los que se han enfrentado los particulares, véase los documentos de trabajo anexo al Informe de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de Las Regiones, de fecha 8.5.2013, «Informe de 2012 sobre la aplicación de la Carta de los Derechos Fundamentales de la UE», COM (2013) 271 final.

derechos y, como consecuencia, de la coexistencia de varias jurisdicciones que habrán de dar solución a las eventuales situaciones de conflicto en su interpretación.[426]

3. LAS DIRECTIVAS EUROPEAS

Las directivas son parte de lo que se denomina Derecho derivado de la Unión o actos legislativos de la Unión.[427] Su objetivo principal —a diferencia de los reglamentos— no es la «unificación» del Derecho, sino la «aproximación de las legislaciones» de los Estado miembros, considerando las peculiaridades de cada uno de ellos. De esta forma se pretenden eliminar las contradicciones entre las disposiciones legislativas y administrativas de los Estados Miembros, o suprimir paso a paso las diferencias con el fin de que en todos los Estados Miembros se impongan, en lo posible, los mismos requisitos materiales en un área determinada.[428]

La Directiva solo es obligatoria para los Estados miembros respecto del objetivo que propone, dejando a su elección la forma y los medios para alcanzar los objetivos establecidos en la Unión. Así, los Estados Miembros pueden tener en cuenta las peculiaridades nacionales a la hora de realizar los objetivos del Derecho de la UE. Al respecto, cabe recordar que las disposiciones de una directiva no sustituyen automáticamente a las del derecho nacional, sino que los Estados miembros están obligados a adecuar su legislación a la normativa de la Unión.[429]

Por regla general, las directivas no confieren derechos ni obligaciones directos a los ciudadanos de la Unión; se dirigen expresamente sólo a los Estados Miembros. En consecuencia, los ciudadanos de la Unión únicamente adquieren derechos y obligaciones a través de los actos de ejecución de la directiva adoptados por las autoridades competentes de los Estados Miembros. Sin embargo, puede ocurrir que en el Estado respectivo no se hubieran producido los actos nacionales de ejecución, o bien, que la

[426] Al respecto véase Teresa PAREJO NAVAJAS, «La Carta de los derechos fundamentales de la Unión Europea», *Derechos y Libertades: Revista de filosofía del derecho y derechos humanos*, n° 22, enero, 2010, pp. 205-239.
[427] Cfr. http://europa.eu/eu-law/decision-making/legal-acts/index_es.htm [Consultado el 08.08.2013]
[428] Para una visión general de la estructura actual de Derecho de la Unión Europa, véase Klaus-Dieter BORCHARDT, *El ABC del Derecho de la Unión Europea* (Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2011), http://bookshop.europa.eu/is-bin/INTERSHOP.enfinity/WFS/EU-Bookshop-Site/es_ES/-/EUR/ViewPublication-Start?PublicationKey=OA8107147. [Consultado el 6.8.2013]
[429] Ibídem, p. 96

transposición fuese deficiente. En tal caso, y de acuerdo a la jurisprudencia del Tribunal de Justicia de la Unión Europea (Comunidades Europeas), el ciudadano de la Unión que resulte perjudicado por la falta de transposición o una transposición deficiente, puede invocar directamente las disposiciones de la directiva, reclamar los derechos previstos en ella y, en su caso, acudir a los tribunales nacionales para asegurar su cumplimiento.[430]

En el ámbito específico de la protección de datos personales, se ha dictado varias Directivas[431], así como Reglamentos y Decisiones que regulan o establecen parámetros comunes a seguir en ciertas áreas específicas que afectan la protección de los datos personales. La revisión de ellas que realizamos a continuación pone el énfasis en el objeto, ámbito de aplicación y particularmente en su relación con el tratamiento de datos por parte de la policía en la prevención y represión de ilícitos penales. El análisis comparativo entre estos instrumentos en relación con sus principios, derechos y obligaciones, cuando sea pertinente, se realizará en los siguientes capítulos esta tesis.

[430] De acuerdo a la jurisprudencia del Tribunal de Justicia, las condiciones para que se produzca este efecto directo son: a) que las disposiciones de la directiva determinen los derechos de los ciudadanos de la Unión o de las empresas de forma suficientemente clara y precisa; b) que el ejercicio del derecho no esté vinculado a ninguna condición u obligación; c) que el legislador nacional no tenga ningún margen de apreciación a la hora de fijar el contenido del derecho; d) que haya expirado el plazo para la transposición de la directiva. Cfr. La STJUE, caso *Francovich y Bonifaci* de 1991, que reconoció la obligación de los Estados Miembros de indemnizar los perjuicios causados por la falta de transposición o por una transposición incorrecta. Klaus-Dieter BORCHARDT, *El ABC del Derecho de la Unión Europea*, op. cit., pp. 97-100.

[431] La primera Directiva sobre protección de datos personales, fue la Directiva 95/46/CE del Parlamento Europeo y Consejo de la Unión Europea, de 24 de octubre de 1995, relativa a *la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*. Luego, le siguieron varias directivas sectoriales que tenían como base común la primera Directiva citada. Entre ellas podemos mencionar: la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, *relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones*; la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de2000, *relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior*; la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio, *relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónica* (Directiva sobre la privacidad y las comunicaciones electrónicas). La anterior Directiva fue modificada por la Directiva 2006/24/CE, del Parlamento y del Consejo, de 15 de marzo, *sobre la conservación de datos generado o tratados en relación con la prestación de servicios de comunicación electrónicas de acceso público o de redes públicas de comunicaciones*; Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009 *por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) no 2006/2004 sobre la cooperación en materia de protección de los consumidores.*

3.1. Directiva 95/46/CE y la propuesta de un nuevo Reglamento General

La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, tiene por objeto establecer normas 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 adelante, la Directiva 95/46/CE).[432] Este instrumento es la pieza fundamental dentro del derecho derivado europeo en materia de protección de los datos personales.[433] En ella se establece el marco general y común del régimen a aplicar en la protección de datos personales en el ámbito de la Unión Europea.[434] Esta necesidad de un marco regulatorio propio de la Unión, se debió esencialmente a que, con anterioridad a la Directiva, muchos países de la Unión, basados en el Convenio 108 del Consejo de Europa, habían dictado leyes sobre protección de datos personales, lo que había

[432] Publicada en el DOCE n° L 281, de 23.11.1995.

[433] La Directiva 95/46/CE, ha sido modificada por el Reglamento (CE) n° 1882/2003 del Parlamento Europeo y del Consejo, publicada en DO n° L 284 de 31.10.2003, p. 1. Sobre la Directiva 95/46/CE existe una abundante bibliografía a la cual nos remitidos para su estudio detallado. Entre otros, véase: Manuel HEREDERO HIGUERAS, *La directiva comunitaria de protección de los datos de carácter personal: comentario a la directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos* (Pamplona: Aranzadi, 1997); Jesús María PRIETO GUTIERREZ, «La Directiva 95/46/CE como criterio unificador», *Revista del Poder Judicial* N° 48 (1998): pp. 165-243; *La protección de los datos personales en el Derecho español* (Madrid: Dykinson, 1999), pp. 295-337; Ana Isabel HERRÁN ORTIZ, *El derecho a la intimidad en la nueva Ley orgánica de protección de datos personales* (Madrid: Dykinson, 2002), pp. 115-194; Lucrecio REBOLLO DELGADO y María Mercedes SERRANO PÉREZ, *Introducción a la protección de datos* (Madrid: Dykinson, 2006), pp. 36-42; María del Carmen GUERRERO PICÓ, *El Impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal* (Thomson Civitas, 2006), pp. 63-101. En lo referido a la adaptación de la legislación española a la Directiva 95/46/CE, véase Raquel CASTAÑO SUÁREZ, «Directiva 95/46, 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: Similitudes y diferencias con la Ley Orgánica 5/1992, de 29 de octubre (LORTAD)», *Noticias de la Unión Europea* n° 162 (1998): pp. 9-16; Manuel HEREDERO HIGUERAS, «Estudio crítico de la transposición de la Directiva 95/46/CE en el ordenamiento jurídico español por la L.O. 15/1999 de 13 de diciembre », *Revista Jurídica de Navarra*, 2001.

[434] Algunos autores plantean que la influencia de la Directiva 95/46/CE va más allá de Europa, ya que se habría transformado de *facto* en un estándar internacional. Se llega a tal conclusión, a partir del artículo 25 de la Directiva, que se refiere a la evaluación del «nivel adecuado» de protección que deben brindan terceros países, para ser destinatarios de transferencias internacionales de datos personales desde la Unión Europea. Plantean que, «si la propia Directiva establece una pléyade de parámetros para evaluar si un tercer país o una solución contractual cumple con "el nivel adecuado", en realidad lo que está planteando es una suerte de estándar». No obstante, agregan, «es un estándar limitado, porque se confiere a un país/organización/destinatario en concreto, y porque tiene que ser examinado y concedido en su caso tras un arduo proceso examinador y deliberativo, caso por caso». De cualquier forma, para ellos la Directiva europea, constituye un "principio de estándar" universal. Cfr. Isabel DAVARA FERNÁNDEZ DE MARCO, *Hacia La Estandarizaciaon de La Protecciaon de Datos Personales: Propuesta Sobre Una "Tercera Vía o Tertium Genus" Internacional*, Temas/La Ley (Madrid: La Ley, 2011), p. 471; C. D. RAAB y C. J. BENNETT, "Protecting Privacy Across Borders: European Policies and Prospects", *Public Administration* Vol. 72 (1994): pp. 95–112.

generado una disparidad normativa entre los Estados Miembros.[435] Era evidente entonces que la sola aplicación del Convenio 108 no garantizaba una protección equivalente de este derecho en los países de la Unión, lo que constituía un problema de cara al objetivo de lograr la libre circulación económica dentro de los países miembros, lo que incluía, el libre tránsito de los datos.[436] De esta forma, la Directiva 95/46 viene a aproximar las legislaciones nacionales de los Estados Miembros de la Unión Europea en cuento al derecho a la protección de datos personales, convirtiéndose hasta la actualidad en el principal instrumento normativo europea de legislación derivada relativo a la protección de datos.[437]

Lo anterior ha contribuido también a la creación de un "orden público comunitario", distinto pero integrado al orden público nacional de los Estados partes, dando lugar al concepto de «espacio europeo de protección». Ahora bien, dentro de los límites del derecho comunitario, pueden surgir disparidades entre los Estados parte respecto de la aplicación de la presente Directiva.[438] En efecto, la Directiva 95/46/CE deja un amplio margen al legislador nacional para adecuar la normativa a sus particularidades locales, pero ello no le resta mérito al carácter homogeneizador de la

[435] Antonio Troncoso, señala al respecto que «la propia Unión Europea ha reconocido como antecedente de su derecho derivado el Convenio 108. Así, la Recomendación de la Comisión de 29 de julio de 1981 instó a los Estados Miembros de la Comunidad a firmar y ratificar lo antes posible el Convenio 108 del Consejo de Europa. De hecho, el propio texto de la Directiva 95/46/CE se basa en los principios enunciados en el Convenio del Consejo de Europa». Agrega que esta necesidad de aproximación normativa entre los países miembros se da sobre todo a partir de los acuerdos de cooperación reforzada suscritos por los Estados Miembros en los ámbito de justicia e interior: «Esto es así especialmente después del reforzamiento de la cooperación en asuntos de justicia e interior, que ha llevado a la celebración de distintos acuerdos entre los Estados Miembros, como el Convenio de Schengen -causa motora principal de la LORTAD-, y que obliga a la transmisión de datos personales entre las Administraciones delos Estados Miembros». Cfr. Antonio TRONCOSO REIGADA, *La protección de datos personales: en busca del equilibrio*, op. cit., pp. 58–59.

[436] Lo anterior, queda de manifiesto en la Exposición de Motivos de la Directiva, dónde señala que es necesario impedir 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» afecten al ordenado funcionamiento del mercado único. Cfr. Considerando 7 de la Directiva 95/46/CE.

[437] Al respecto María Mercedes Serrano, señala que con carácter general «puede decirse que la Directiva mejora la regulación contenida en el Convenio, haciéndolo constar así expresamente. Pero además, la Directiva no es una norma de mínimos al estilo de aquél. Según su art. 1.2: "los Estados Miembros no podrán restringir la libre circulación de datos de carácter personal asegurando así la protección del individuo". La norma comunitaria concreta un alto nivel de protección, más fuerte que el señalado por el Convenio que dejaba a disposición de los Estados parte la posibilidad de ser mejorado.» Cfr. SERRANO PÉREZ, *El derecho fundamental a la protección de datos. Derecho español y comparado*, p. 95. En el mismo sentido, REBOLLO DELGADO y SERRANO PÉREZ, *Introducción a la protección de datos*, p. 37.

[438] Cfr. Considerando 9 de la Directiva 95/46/CE.

legislación de los diferentes Estados Miembros de la Unión.[439] Además, la Directiva 95/46/CE se ha aplicado con carácter supletorio respecto de las Directivas posteriores, que se han dictado en diversos ámbitos, incluido el antiguo tercer pilar comunitario. Atendido este doble carácter, homogeneizador y supletorio, la Directiva ha contribuido a la instalación, no tanto de un territorio comunitario de protección, sino de un territorio de protección europeizado.[440]

La Directiva 95/46/CE tiene por objetivo conciliar dos bienes o valores jurídicos esenciales para la Unión. Por un lado, la protección de los derechos y libertades fundamentales de las personas físicas, y particularmente el derecho a la intimidad (vida privada) respecto del tratamiento de los datos personales; y por otro, asegurar la libre circulación de datos personales entre los Estados Miembros.[441] Se trata, pues, de impedir que las diferencias entre los niveles de protección de los derechos y libertades de las personas, incluidos los datos personales, afecte el funcionamiento del mercado único. Por tanto, detrás del objetivo de equivalencia material de los regímenes nacionales de protección de datos personales de los Estados parte que persigue la Directiva, subyace un interés de integración económica vinculado a la realización del mercado interior.[442]

Cabe recordar que al momento de elaborarse la Directiva 95/46/CE, no existía la Carta de Derechos Fundamentales de la Unión Europea y, por tanto, el derecho a la protección de datos personales no se había reconocido aún como un derecho fundamental autónomo en el Derecho originario ni derivado de la Unión Europea.[443] Es por ello que los artículos y considerados de la Directiva hacen referencia indistintamente al «derecho a la intimidad» y al «derecho al respeto de la vida privada» reconocido en el artículo 8 del Convenio Europeo para la Protección de los Derechos

[439] En el caso de España, la Directiva fue transpuesta al derecho interno por medio de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Publicada en el BOE núm. 298 de 14.12.1999.

[440] Recuérdese el ámbito material de aplicación de este instrumento va más allá de la Unión, extendiéndose al Espacio Económico Europeo. Al respecto véase Diana SANCHO VILLA, *Transferencia internacional de datos personales* (Pamplona: Civitas, 2003), p. 60.

[441] Cfr. los Considerandos y el artículo 1de la Directiva 95/46/CE. Cabe recordar que al momento de la elaboración de la Directiva 95/46/CE el derecho fundamental a la protección de datos no se había reconocido como un derecho fundamental autónomo en el derecho originario de la Unión.

[442] Ricard MARTÍNEZ MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa*, p. 224.

[443] La CDFUE, que reconoce en su artículo 8 el derecho a la protección de datos personales, fue proclamada en Niza el año 2000.

Humanos y de las Libertades Fundamentales, así como en los principios generales del Derecho comunitario, como soporte *iusfundamental* de la Directiva.[444]

En cuanto al contenido de la Directiva 95/46, esta se estructura en 32 artículos que se distribuyen en VII capítulos.[445] El capítulo I establece disposiciones generales (objeto de la Directiva, definiciones, ámbito de aplicación y el derecho nacional aplicable)[446]. El capítulo II, se divide, a su vez, en varias secciones: en la primera sección se establecen los principios relativos a la calidad de los datos (artículo 6); la segunda sección se destina a las condiciones necesarias para la legitimidad del tratamiento (artículo7)[447]; la tercera sección se dedica al tratamiento de datos especialmente sensibles (artículo 8) y al tratamiento de datos personales con fines periodísticos, de expresión artística o literaria (artículo 9); la sección cuarta del capítulo II se dedica a regular el derecho a la información del interesado (artículos 10 y 11); la sección V se destina normar el derecho de acceso (artículo 12); las excepciones y limitaciones a los derechos en la sección VI (artículo 13); la sección VI, se dedica al derecho de oposición (artículo 14) y las dediciones automatizadas (artículo 15); las secciones VIII y IX se destinan a regular las obligaciones de seguridad, confidencialidad y notificación a la autoridad de control, control previo y publicidad de los tratamientos (artículos 16 a 21). El capítulo III se destina a regular los recursos judiciales, responsabilidades y sanciones (artículo 22 a 24). El capítulo IV regula las transferencias de datos personales a terceros países (artículos 25 y 26). El capítulo V se destina a los códigos de conducta (artículo 27); el capítulo VI se destina las autoridades

[444] Cfr. Considerandos 2, 7, 9, 11, 10, 33, 34, 68; y artículos 1; 9, 13.2, 25.6, 26.2 y 3 de la Directiva 95/46/CE. En el mismo sentido véase MARTÍNEZ MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa*, p. 224.

[445] Además, cuenta con 72 considerandos, imprescindibles para la adecuada interpretación de sus disposiciones.

[446] Al respecto véase Lucrecio REBOLLO DELGADO, *Derechos fundamentales y protección de datos* (Madrid: Dykinson, 2004), p. 132.

[447] Véase Lucrecio REBOLLO DELGADO, *Vida privada y protección de datos en la Unión Europea*, pp. 114-117. Un punto interesante sobre los principios de la Directiva, dice relación sobre la preeminencia de algunos de ellos como criterio rector de la misma. Existen posiciones encontradas al respecto. Así, para Ricard Martínez, «El núcleo central de la protección otorgada por la Directiva se basa en el consentimiento, en la garantía de la autodeterminación individual, sin perjuicio de la existencia de supuestos en los que una habilitación legal, los derechos e intereses legítimos de terceros o el propio interés vital del titular de los datos, habiliten para un tratamiento de datos sin consentimiento»; en cambio, para María del Carmen Guerrero «El centro de gravedad del sistema instaurado por la Directiva 95/46/CE se desplaza a las condiciones de licitud del tratamiento, a diferencia de la propuesta de 1990, que daba mayor relevancia al papel jugado por el consentimiento». Cfr. GUERRERO PICÓ, *El Impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, p. 76; y Ricard MARTÍNEZ MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa*, p. 225.

de control y el grupo de protección (artículo 28 a 30); el capítulo VII regulas las medidas de ejecución de la Directiva (artículo 31); y las disposiciones finales sobre cumplimiento de la Directiva (artículos 32 a 34) .

En cuanto al ámbito material de aplicación, la Directiva 95/46/CE se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado (manual) de datos personales contenidos o destinados a ser incluidos en un fichero, realizado en el ámbito de aplicación del derecho comunitario.[448] Como se puede apreciar, el ámbito de aplicación material de la Directiva es bastante amplio, ya que contempla cualquier tipo de información personal y en cualquier formato. Por tanto, no sólo se trata de abarcar el empleo de bases de datos o soportes lógicos que contengan información alfanumérica, sino también aquellos que integren información estructurada en soporte papel, o información consistente en imágenes y sonidos[449]. Además se prevé la posibilidad de una aplicación restringida de la Directiva a este último tipo de información cuando sea utilizada con fines periodísticos, literarios o por el sector audiovisual. Se trataría, en este último caso, de hacer compatible el ejercicio el derecho a la libertad de expresión y el derecho a la información con las garantías previstas por la Directiva.[450]

La Directiva, bajo la antigua lógica de división de pilares comunitarios, estableció una serie de materias que quedan excluidas de su campo de aplicación material. Así pues, sus normas no se aplican al tratamiento de datos personales que se efectúen en el ejercicio de actividades no comprendidas en el ámbito de aplicación del derecho comunitario —antiguo primer pilar comunitario— como tampoco a las materias previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea —antiguo segundo y tercer pilar comunitario— y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado

[448] Cfr. Artículo 3.1. de la Directiva.
[449] Cfr. Considerando 14 de la Directiva. No obstante, los tratamientos de datos constituidos por sonido e imagen, como los de la vigilancia por videocámara, no están comprendidos en el ámbito de aplicación de la presente Directiva cuando se aplican con fines de seguridad pública, defensa, seguridad del Estado o para el ejercicio de las actividades del Estado relacionadas con ámbitos del derecho penal o para el ejercicio de otras actividades que no están comprendidos en el ámbito de aplicación del Derecho comunitario. Cfr. Considerandos 16.
[450] Cfr. Considerando 37 y artículo 9 de la Directiva. Al respecto véase Ricard MARTÍNEZ MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa*, p. 225.

con la seguridad del Estado), y las actividades del Estado en materia penal.[451] Por tanto, la Directiva 95/46 excluye de su ámbito de aplicación los datos policiales.[452] También se excluye de su ámbito de aplicación material el tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;[453] el tratamiento referido a personas jurídicas;[454] así como las carpetas y conjuntos de carpetas que no estén estructuradas conforme a criterios específicos.[455]

Por su parte el Artículo 13 de la Directiva citada, regula las excepciones y limitaciones de los derechos y obligaciones en materia de protección de datos, permitiendo dichas restricciones, entre otros casos, para la salvaguardia de la seguridad del Estado, la defensa, la seguridad pública, la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas.[456] Estas excepciones y limitaciones deben interpretarse de acuerdo con lo dispuesto en el artículo 8 del CEDH. Hasta ahora estas restricciones se habían interpretado como cubriendo los supuestos de datos recogidos en el ámbito del primer pilar (actividades económicas), cuya utilización es necesaria en el ámbito del tercer pilar.[457]

Por último, cabe hacer presente que el artículo 16.2 del TFUE obliga al legislador europeo a establecer normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Para ello, la Comisión ha propuesto una serie de importantes reformas a las normas de la Unión Europea en

---

[451] Cfr. los Considerandos 13, 16, 43; los artículos 3.2 y 13 de la citada Directiva.
[452] En el mismo sentido, Joaquín BAYO DELGADO, «La cooperación policial internacional a la luz de la Propuesta revisada de Decisión Marco relativa a la protección de datos», op. cit., p. 24.
[453] Cfr. Considerando 12 de la Directiva.
[454] Cfr. Considerando 14 de la Directiva.
[455] Cfr. Considerando 27 de la Directiva.
[456] El Artículo 13.1 señala que «Los Estados Miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de: a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas; e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales; f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e) ; g) la protección del interesado o de los derechos y libertades de otras personas.
[457] Joaquín BAYO DELGADO, op. cit., pp. 24-25. Al respecto véase *infra* aparatado 3.2 del capítulo quinto, sobre la polémica generada en relación a la Directiva 2006/24/CE, por la utilización de los datos personales de los usuarios de los servicios de comunicaciones electrónicas con fines de prevención y represión penal.

materia de protección de los datos personales, que pretenden actualizar y modernizar los principios consagrados en la Directiva de 1995, para garantizar el derecho a la protección de los datos personales en el futuro.[458] Estas reformas buscan, entre otros temas: incrementar la responsabilidad y la obligación de rendir cuentas de todos aquellos que procesan los datos personales; reforzar el papel de las autoridades nacionales independientes con competencias en la materia; introducir el derecho al olvido, respecto de los datos en línea; ampliar los principios y normas generales en materia de protección de datos a las administraciones nacionales de policía y justicia penal.[459] Para darle una mayor legitimidad democrática al proceso de revisión de la Directiva 95/46/CE se consultó a todas las partes interesadas (operadores del sistema)[460], así como también a los ciudadanos europeos.[461] También se tuvieron a la vista varios estudios[462] y Dictámenes, tanto del GT29[463], como del Supervisor Europeo de Protección de Datos[464], y un estudio de impacto de las distintas opciones

[458] Al respecto véase COM (2012) 9 final, «La protección de la privacidad en un mundo interconectado – Un Marco Europeo de Protección de Datos para el siglo XXI»; COM (2012) 10 final, «la Propuesta de Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos»; COM(2012) 11final, «la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos».

[459] Cfr. Informe de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 8 de mayo de 2013; y el «Informe de 2012 sobre la aplicación de la Carta de los Derechos Fundamentales de la UE. COM (2013) 271 final», p. 3.

[460] La consulta con todas las partes interesadas sobre la revisión del actual marco jurídico para la protección de datos de carácter personal, incluyó dos fases: la primera se realizó entre el 9 de julio y el 31 de diciembre de 2009, y se denominó precisamente *Consulta sobre el marco jurídico para el derecho fundamental a la protección de datos de carácter personal*. La Comisión recibió 168 respuestas, 127 de personas físicas, organizaciones y asociaciones empresariales, y 12 de autoridades públicas. La segunda fase, se desarrolló del 4 de noviembre de 2010 al 15 de enero de 2011, *Consulta sobre el enfoque global de la Comisión sobre la protección de datos de carácter personal en la Unión Europea*. En esta etapa, la Comisión recibió 305 respuestas, de las cuales 54 procedían de ciudadanos, 31 de autoridades públicas y 220 de organizaciones privadas, especialmente de asociaciones empresariales y organizaciones no gubernamentales. Las respuestas no confidenciales pueden consultarse en el sitio internet de la Comisión: http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm. y http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm. [Consultado el 08.08.2013]

[461] Eurobarómetro espacial (EB) 359, *Protección de datos e identidad electrónica en la UE*, realizado entre noviembre y diciembre de 2010. Publicado en 2011 y disponible en http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

[462] Véase el estudio sobre las ventajas económicas de las tecnologías potenciadoras de la privacidad y el estudio comparativo de los distintos enfoques ante los nuevos retos en materia de protección de la privacidad, en particular a la luz de los avances tecnológicos, de enero de 2010. Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf

[463] Sus Dictámenes se pueden consultar en http://ec.europa.eu/justice/protección de datos/article-29/documentation/index_en.htm. Sobre el grupo de trabajo creado por el artículo 29 de la Directiva 95/46/CE véase el capítulo X.X de este trabajo..

[464] Sus Dictámenes están disponibles en el sitio internet del SEPD: http://www.edps.europa.eu/EDPSWEB/. Sobre el Supervisor Europeo de Protección de Datos, véase el capítulo X.X de este trabajo.

planteadas.[465] Estas propuestas de reformas han contado con el apoyo político del Parlamento Europeo, el Consejo de la Unión Europea, y del Comité Económico y Social Europeo.[466]

3.2. Directiva 2006/24/CE

Con posterioridad a la Directiva 95/46/CE, se han dictado una serie de Directivas sectoriales. La primera de ellas fue la Directiva 97/66/CE de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.[467] Con el objeto de actualizar su contenido de acuerdo con el desarrollo de las tecnologías, ésta Directiva fue derogada y sustituida por la Directiva 2002/58/CE del Parlamento y del Consejo, de 12 de julio, 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).[468] Por último, la Directiva 2002/58/CE fue modificada por la Directiva 2006/24/CE, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones.[469] Esta última Directiva, fue objeto de varios cuestionamientos durante su vigencia, hasta que finalmente el Tribunal

[465] Véase el Dictamen emitido por Comité de Evaluación de Impacto (CEI), de 9 de septiembre de 2011.A raíz del dictamen del CEI, se aclararon los objetivos del marco jurídico en vigor; en la sección consagrada a la definición de problemas se añadieron más elementos de prueba y explicaciones/aclaraciones adicionales.

[466] Cfr. . Resolución del Parlamento Europeo, de 6 de julio de 2011, «sobre un enfoque global de la protección de los datos personales en la Unión Europea», (2011/2025(INI); Las Conclusiones del Consejo de la Unión Europea, de 24 de febrero de 2011, en las que respalda en términos generales la intención de la Comisión de reformar el marco de la protección de datos; y CESE 999/2011.

[467] Publicada en el DOCE n° L 24 de 30.01.1998 pp. 1-8. Al respecto véase Antonio PRIETO ANDRÉS, «La nueva directiva europea sobre el tratamiento de datos personales y la protección de la intimidad en el sector de las telecomunicaciones», *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía* n.º 5 (2002): pp. 1710-1713; Ricard MARTÍNEZ MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa*, pp. 226-230; Lucrecio REBOLLO DELGADO, *Derechos fundamentales y protección de datos*, pp. 138-139; María del Carmen GUERRERO PICÓ, *El Impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, p. 94 y el Capítulo III del mismo libro.

[468] Publicada en el DOCE n° L 2001/37, de 31.07.2002. Esta Directiva, a diferencia de la 95/46/CE y 97/66/CE, hace una referencia expresa no sólo a la necesidad de proteger la intimidad y la vida privada de los ciudadanos, sino al derecho fundamental a la protección de datos personales como derecho autónomo. Al respecto véase Antonio TRONCOSO REIGADA, *La protección de datos personales: en busca del equilibrio* (Tirant lo Blanch, 2010), p. 60; Ricard MARTÍNEZ MARTÍNEZ, *Una aproximación crítica a la autodeterminación informativa* (Madrid: Thomson-Civitas, 2004), pp. 230-232; Lucrecio REBOLLO DELGADO, *Derechos fundamentales y protección de datos* (Madrid: Dykinson, 2004), pp. 139-140.

[469] Publicada en el DOUE n° L 105, de 13.04.2006, p. 54-63.

de Justicia de la Unión Europea la invalidó en abril de 2014, como pasamos a revisar a continuación.

3.2.1. El cuestionamiento a su base jurídica

En una primera etapa, la utilización del artículo 95 del TCE como base jurídica de la Directiva 2006/24/CE fue cuestionada, atendido el objeto y ámbito de aplicación de la misma. En efecto, la finalidad perseguida por éste instrumento normativo era garantizar la disponibilidad de los datos tratados por los proveedores de servicios de comunicaciones electrónicas con fines de investigación, detección y enjuiciamiento de delitos graves[470]; y su ámbito de aplicación son los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado, excluyendo el contenido de las comunicaciones electrónicas.[471] Como se puede apreciar, existiría una aparente incongruencia entre el fin declarado por la Directiva, esto es, la prevención y represión penal (propio del antiguo tercer pilar comunitario) y la basa jurídica elegida para su aprobación, sustentada en el desarrollo del mercado interior (propia del antiguo primer pilar comunitario).[472]

Lo anterior, llevó a Irlanda en julio de 2006 a iniciar un proceso ante el TJCE con el fin de lograr la anulación de la Directiva 2006/24/CE, fundado en que la misma no había sido adoptada sobre la debida base jurídica. Dicha acción fue desestimada por el tribunal al considerar que la Directiva en cuestión se justificaba en la necesidad de

[470] En efecto, del artículo 1.1 y los considerandos 4, 5, 7 y 11, 21 y 22 de la Directiva 2006/24, queda claro que el principal objetivo de esta Directiva es la armonización de las disposiciones de los Estados miembros relativas al mantenimiento, por parte de proveedores de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicación, de determinados datos generados o tratados por los mismos, a fin de garantizar que los datos están disponibles para el propósito de la prevención, investigación, detección y enjuiciamiento de delitos graves, como la delincuencia organizada y el terrorismo, en cumplimiento de los derechos establecidos en los artículos 7 y 8 de la Carta.

[471] Cfr. Artículo 1.2 de la Directiva.

[472] Una opinión más radical manifiesta Mónica VILASAU SOLANA, quién señala que «Mediante la Directiva 2006/24 se están socavando los principios de protección de datos sentados en la UE. En definitiva, las medidas adoptadas en la presente Directiva superan totalmente los beneficios que se puedan obtener con la misma ya que se instaura una filosofía de sospecha y vigilancia de todos los ciudadanos sin un mínimo indicio. Además, ya de forma directa, ya indirecta, son los propios usuarios quienes acabarán soportando los costes de las medidas adoptadas». Cfr. «La Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. privacidad.», *IDP: revista de Internet, derecho y política = revista d'Internet, dret i política* n.º 3 (2006): pp. 1-15.

una norma armonizadora de las legislaciones nacionales de los Estados Miembros sobre conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas, actividad que consideró como relevante y de impacto directo en el mercado interior.[473] Con ello el TJCE quiso desmarcarse de una posible comparación con la sentencia emitida pocos meses antes, el 30 de mayo de 2006, referente al Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre transferencia de los datos personales contenidos en los registros de nombres de los pasajeros de la compañías aéreas europeas con destino o que sobrevolaran territorio norteamericano, las cuales debían transferir al Servicio de Aduanas y Protección de Fronteras de los Estados Unidos de América todos los datos personales de los pasajeros.[474]

3.2.2. La invalidación por parte del TJUE

En una segunda etapa, la postura del TJUE sobre la materia en estudio, cambia radicalmente con el pronunciamiento realizado con fecha 08 de abril de 2014, donde el máximo tribunal de la Unión Europea invalidó la Directiva 24/2006.[475] En esta oportunidad, y en razón de dos requerimientos prejudiciales presentados por la *High Court* de Irlanda y la *Verfassungsgerichtshof* de Austria, se pide al Tribunal europeo examinar la validez de la Directiva 2006/24 a la luz de Los artículos 7, 8 y 11 de la Carta de Derechos Fundamentales de la Unión Europea.

En éste último fallo, el TJUE se pronunció, entre otras materias sobre: si los datos de los abonados y usuarios registrados puede ser retenidos con fines de seguridad; si la Directiva 24/2006 cumple con los requisitos sobre protección de datos personales que derivan del artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea; sobre la validez de la Directiva a la luz del artículo 7 de la misma Carta (vida privada); las condiciones en que la Unión Europea puede establecer una limitación al ejercicio de

[473] Cfr. STJCE, caso *Irlanda vs. Parlamento y Consejo*, de 29 de febrero de 2009.
[474] Cfr. SSTJCE, casos (C-317/04) y (C-318/04), *Parlamento Europeo vs Consejo de la Unión Europea y Comisión de las Comunidades Europeas*), ambas de 30 de mayo de 2006. Al respecto véase Joan Lluís PÉREZ FRANCESCH, Tomás GIL y Alejandro GACITÚA ESPÓSITO, "Informe sobre el PNR. La utilización de datos personales contenidos en el registro de nombres de pasajeros: ¿fines represivos o preventivos?", *Institut de Ciències Polítiques i Socials* 297, Working papers (2011): pp. 1-27.
[475] Cfr. SSTJUE, en los casos acumulados (C-293/12), *Digital Rights Ireland* y (C-594/12), *Seitlinger y otros.* El fallo está disponible en su versión en inglés, en el sitio: http://www.janalbrecht.eu/fileadmin/material/Dokumente/c_293_c_594.pdf [Consultado el 17.4.2014]

los derechos fundamentales, en el sentido del artículo 52, apartado 1, de la CDFUE mediante una directiva y sus medidas nacionales de transposición.[476]

Para el máximo Tribunal Europeo, algunas disposiciones de la Directiva 2006/24 vulneran las normas relativas al respeto de la vida privada y las comunicaciones previstas en el artículo 7, así como la protección de datos personales de acuerdo con el artículo 8 de la CDFUE. Sobre éste último punto, el TJUE, señala que la retención de datos y el acceso por parte de las autoridades nacionales habilitadas a los mismos, en los términos del artículo 5 de la Directiva 2006/24, constituye una excepción al régimen general de protección establecido por las Directivas 95/46 y 2002/58 en lo que respecta al tratamiento de datos personales en el sector de las comunicaciones electrónicas, ya que éstas directivas «establecen la confidencialidad de las comunicaciones y de los datos de tráfico, así como la obligación de borrar o hacer que esos datos anónimos cuando ya no son necesarios para el propósito de la transmisión de una comunicación, a menos que sean necesarios para la facturación y sólo por el tiempo que sea necesario».

Cabe recordar que el artículo 3 de la Directiva 2006/24, establecía que los proveedores de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones debían retener los datos enumerados en el artículo 5 de la Directiva con el fin de que sean accesibles, de ser necesario, las autoridades nacionales competentes.[477] Si bien, la Directiva excluía el contenido de las comunicaciones de los datos a retener o conservar, ellos permitían en su conjunto extraer conclusiones muy precisas en relación con la vida privada de las personas, tales como los hábitos de la vida cotidiana, los lugares permanentes o temporales de residencia, los movimientos de una persona, las actividades llevadas a cabo, las relaciones y entornos sociales

[476] Cabe señalar que la transposición de la Directiva 2006/24 ha dado lugar a varios recursos por incumplimiento y que aún está pendiente un recurso basado en el artículo 260 TFUE, apartado 3. Cfr. asunto (C‑329/12), Comisión vs Alemania.

[477] Entre los datos mencionados en el artículo 5, se encontraban: los datos necesarios para rastrear e identificar el origen de una comunicación y su destino, para identificar la fecha, hora, duración y tipo de comunicación, para identificar el equipo de comunicación de los usuarios, y para identificar la localización del equipo de comunicación móvil, los datos que constan , entre otros, el nombre y la dirección de del abonado o usuario registrado , el número de teléfono de llamada , el número llamado y una dirección IP para los servicios de Internet. Como lo reconoce el fallo del TJUE «Los datos mencionados en el artículo 5, permitían, en particular, conocer la identidad de la persona con la que un abonado o usuario registrado se ha comunicado y por qué medios, identificar el momento de la comunicación, así como el lugar desde el que esa comunicación se llevó a cabo. También hacen que sea posible conocer la frecuencia de las comunicaciones del abonado o usuario registrado con otras personas durante un período determinado». Cfr. STJUE C-293/12, considerando 26 [Traducción nuestra].

frecuentados por las personas. Siguiendo la Opinión del Abogado General, el TJUE califica la injerencia causada por la Directiva 2006/24 en los derechos fundamentales a la vida privada (artículo 7) y a la protección de datos (artículo 8) establecidos en la CDFUE como de «amplio alcance» y «particularmente grave».[478] Además, agrega el tribunal «el hecho de que los datos sean retenidos y posteriormente utilizados sin que el abonado o usuario registrado sea informado es probable que genere en la mente de las personas interesadas la sensación de que su vida privada es objeto de una vigilancia constante».[479]

No obstante reconocer la existencia de las injerencias en los derechos garantizados por los artículos 7 y 8 de la Carta, el Tribunal también reconoce que dichos derechos pueden ser objetos de limitación y restricciones, por lo que se limita a verificar si dichas limitaciones al ejercicio de estos derechos y libertades fundamentales cumplen con lo dispuesto por el artículo 52.1.[480] En consecuencia, el TJUE, se avoca a analizar si las limitación que contempla la Directiva 2006/24 respecto del ejercicio de los derechos y libertades reconocidos por los artículos 7 y 8 de la Carta, respetan o no el contenido esencial de dichos derechos. Asimismo, analiza la proporcionalidad de la medida, y si dichas limitaciones son 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.[481]

Por lo que se refiere a la afectación de la esencia de los derechos a la vida privada y a la protección de datos, el tribunal concluye que la Directiva no afecta el derecho fundamental a la intimidad y los demás derechos establecidos en el artículo 7 de la Carta, ya que «a pesar de que la retención de los datos requeridos por la Directiva

[478] Ibídem, considerando 35 y 36. En este punto, el TJUE, sigue los criterios establecidos por la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH), y cita en relación al artículo 8 del CEDH los casos: *Leander* contra Suecia, 26 de marzo de 1987 § 48; *Rotaru* contra Rumania [GS], núm 28341/95, § 46; y *Weber y Saravia* contra Alemania (diciembre), no 54934/00, § 79. Véase también los apartados 77 y 80 de las Conclusiones del Abogado General, Pedro CRUZ VILLALÓN sobre los asuntos C‑293/12 y C-594/12, de fecha el 12.12. 2013.

[479] Cfr. STJUE C-293/12, considerando 35 [traducción nuestra] y los apartados 52 y 72 de la Opinión del Abogado General.

[480] STJUE C-293/12, considerando 38.

[481] El Artículo 52.1 de la CDFUE dispone que «cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás».

2006/24 constituye una interferencia especialmente grave con esos derechos, no es tal como para afectar negativamente el contenido esencial de dichos derechos, dado que, como se desprende del artículo 1.2, la Directiva no permite la adquisición de conocimientos sobre el contenido de las comunicaciones electrónicas».[482] En la misma lógica, el TJUE, concluye que la Directiva tampoco afecta negativamente la esencia del derecho fundamental a la protección de los datos personales recogidos en el artículo 8 de la Carta, «ya que el artículo 7 de la Directiva 2006/24 establece, en relación con la protección de datos y los datos seguridad, que, sin perjuicio de las disposiciones adoptadas en virtud de las Directivas 95/46 y 2002/58, ciertos principios de protección de datos y seguridad de los datos deben ser respetadas por los prestadores de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones. Según estos principios, los Estados miembros deben velar por que las medidas técnicas y organizativas adecuadas que se adopten contra la destrucción accidental o ilícita, la pérdida accidental o alteración de los datos».[483] Al respecto, creemos que el tribunal se limitó a constatar el cumplimiento formal o declarado de la Directiva, pero no entró al análisis material, en el sentido de verificar si efectivamente dichos principios fueron cumplidos por los sujetos pasivos de la Directiva, esto es, por las autoridades nacionales habilitadas para el tratamiento de dichos datos con fines de seguridad pública y que se encuentran obligadas a dar cumplimiento a los principios y obligaciones consagrados en ella.

En cuanto a la cuestión de si esa injerencia satisface un **objetivo de interés general**, el Tribunal señala que mientras la Directiva 2006/24 declara que su objetivo es armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores con respecto a la conservación de determinados datos generados o tratados por los mismos, el objetivo material de dicha Directiva es, como se desprende del artículo 1.1 de la misma, garantizar que dichos datos estén disponibles para fines de investigación, detección y enjuiciamiento de delitos graves, según lo definido por cada Estado miembro en su legislación nacional. Por tanto, el objetivo material de dicha Directiva es, en última instancia, a la seguridad pública.[484] Pues bien, siguiendo la jurisprudencia del Tribunal, el tribunal concluye que, tanto la lucha contra el terrorismo

[482] STJUE C-293/12, considerando 39 [traducción nuestra].
[483] Ibídem, considerando 40 [traducción nuestra].
[484] Ibídem, considerando 41 [Traducción nuestra].

internacional con el fin de mantener la paz y la seguridad internacionales[485], como la lucha contra los delitos graves, a fin de garantizar la seguridad pública constituyen un objetivo de interés general.[486] Por otra parte, agrega el tribunal, hay que señalar a este respecto, que el artículo 6 de la Carta establece el derecho de cualquier persona, no sólo a la libertad, sino también a la seguridad.[487] Por consiguiente, el máximo tribunal europeo resuelve que la retención de los datos con el fin de permitir que las autoridades nacionales competentes el acceso a esos datos, como exige la Directiva 2006/24, satisface un objetivo de interés general.[488]

Establecido que la Directiva cumple un objetivo de interés general, el TJUE se avoca a verificar si la injerencia en los derechos fundamentales afectados cumple con el principio de proporcionalidad.[489] A este respecto, según la jurisprudencia reiterada del Tribunal de Justicia, el principio de proporcionalidad exige que los actos de las instituciones de la UE sean aptos para alcanzar los objetivos legítimos perseguidos por la normativa controvertida y no excedan los límites de lo que es resulta apropiado y necesario para alcanzar dichos objetivos.[490] Por tanto, el grado de discrecionalidad del legislador europeo se encuentra limitado, ya que el tribunal puede revisar el cumplimiento de dichas condiciones.[491] En el caso en estudio, teniendo en cuenta el importante papel desempeñado por la protección de los datos personales a la luz del derecho fundamental al respeto de la vida privada y la extensión y gravedad de la interferencia con ese derecho causado por la Directiva 2006/24, la discreción del legislador de la Unión se reduce y, por tanto, la revisión debe ser estricta. El TJUE,

---

[485] En este sentido, véase las sentencias del TJUE en los casos *Kadi y Al Barakaat International Foundation* vs *Consejo y Comisión de la UE* (402/05 P) y (C-415/05 P) C: 2008:461, párrafo 363; y casos *Al-Aqsa v Consejo de la UE* (*C*-539/10 P) y (C-550/10 P) C: 2012:711, párrafo 130.

[486] En este sentido, véase la sentencia TJUE C-145/09 *Tsakouridis* UE: C: 2010:708, apartados 46 y 47.

[487] STJUE 293/12, párrafo 41 [Traducción nuestra].

[488] Ibídem, párrafo 44. En este sentido el Tribunal señala que por la creciente importancia de los medios de comunicación electrónica, la retención de los datos que puede constituir una herramienta valiosa ser retenidos en virtud de la Directiva a fin de permitir a las autoridades nacionales competentes en materia penal que tengan oportunidades adicionales para esclarecer los delitos graves. En consecuencia, el Tribunal señala que «la retención de estos datos se puede considerar como apta para alcanzar el objetivo perseguido por dicha Directiva». Cfr. párrafo 49.

[489] Ibídem, párrafo 45.

[490] Ibídem, párrafo 46. En el mismo sentido, véase: asunto *Afton Chemical UE*, C-343/09, apartado 45; *Volker und Markus Schecke y Eifert* UE: C: 2010:662 párrafo 74; los casos *Nelson y otros*, C-581/10 y C-629/10: C: 2012:657, apartado 71; y las sentencias *Sky Österreich* C-283/11 U: C: 2013:28, apartado 50, y Caso *Schaible UE:*C -101/12 C: 2013:661, apartado 29.

[491] STJUE 292/12, párrafo 47. En el mismo sentido véase, por analogía, en relación con el artículo 8 del CEDH, el fallo del TEDH en el caso *S. y Marper* contra el Reino Unido [GC], núms. 30562/04 y 30566/04, § 102.

luego de un detallado análisis, concluye que el legislador de la Unión Europea al adoptar la Directiva 2006/24, ha excedido los límites impuestos por el respeto del principio de proporcionalidad a la luz de los artículos 7, 8 y 52 (1) de la Carta.[492]

Como se puede apreciar, a diferencia del caso anterior de 2006, aquí los cuestionamientos no se formulan en razón de la base jurídica utilizada para la elaboración de la directiva, ni sobre la finalidad perseguida por la misma, sino sobre la proporcionalidad de la medida y las condiciones en que las directivas europeas pueden establecer limitaciones a los derechos fundamentales reconocidos por la CDFUE.[493]

Como reflexión final sobre este apartado, podemos constatar, por una parte, la dificultad que revestía encuadrar algunas normas europeas en alguno de los extintos pilares comunitarios, atendido que varias de las directivas y reglamentos excedían de lo estrictamente necesario para el desarrollo del mercado interior y pasaban a regular materias propias de la prevención y represión penal del antiguo tercer pilar comunitario. Por otra parte, y no menos importante, se evidencia una tendencia cada vez mayor a que las autoridades públicas europeas exijan a compañías privadas la entrega o el acceso a los datos personales que consten en sus registros, todo ello bajo el amplio concepto del resguardo de la seguridad nacional.[494] Con este nuevo fallo del TJUE, al parecer hemos entrado a un nuevo ciclo, donde la defensa de las libertades fundamentales sirven nuevamente de cortafuego a medidas de prevención general penal, que pretenden evitar la intromisión desproporcionada en la privacidad de las personas por razones de seguridad. Creemos que ello se encuentra en línea con las directrices generales de las nuevas propuestas de Directiva y Reglamento sobre protección de datos que se discuten actualmente en el Parlamento europeo, las que sin perjuicio de sus falencias, contienen una propuesta más equilibrada entre seguridad y libertad.

[492] STJUE, C-293/12, párrafo 69.
[493] Al respecto, resulta muy ilustrativo la Opinión del Abogado General Pedro CRUZ VILLALÓN, presentadas el 12 de diciembre de 2013, sobre los asuntos C‑293/12 y C-594/12. Disponible en http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d6ac60300fd67a41bd866d9effc6845a39.e34KaxiLc3eQc40LaxqMbN4OaNeMe0?text=&docid=145562&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=259034 [Consultado el 17.4.2012].
[494] En esta línea encontramos los Acuerdos de Puerto Seguro, PNR y SWIFT.

3.3. Reglamento 45/2001 relativo al tratamiento de datos personales por las instituciones y los organismos comunitarios

El Reglamento 45/2001, de 18 de diciembre de 2000, relativo al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (en adelante, el R45/2001)[495] al igual que las Directivas analizadas precedentemente, tiene un doble fin. Por una parte, que las instituciones y organismos comunitarios garanticen la protección efectiva de los derechos y las libertades fundamentales de las personas físicas, y en particular su derecho a la intimidad, en lo que respecta al tratamiento de los datos personales; y por otra, que dichos organismos e instituciones no limiten ni prohíban la libre circulación de datos personales entre ellos o entre ellos y destinatarios de los Estados Miembros.[496] Para supervisar el cumplimiento de sus disposiciones se crea la figura del «Supervisor Europeo de Protección de Datos».[497]

El R45/2001, se aplica exclusivamente al tratamiento de datos personales por parte de todas las instituciones y organismos comunitarios, en el ámbito de aplicación del derecho comunitario, esto es, del antiguo primer pilar comunitario.[498] Por tanto, en principio, toda la actividad realizada por organismos públicos europeos encargados de la prevención y represión penal estarían excluidos del ámbito de aplicación del Reglamento. No obstante, si se analizan las disposiciones vigentes de Europol, Eurojust, así como de los grandes sistemas de información que actualmente se utilizan para la prevención de ilícitos transnacionales a nivel europeo (SIS, VIS, EURODAC, entre

---

[495] Publicado en el DOCE n° L 8 de 12.1.2001, p. 1-22. Sobre el Reglamento 45/2001 véase Eugenio ULL PONT, *Derecho Público de la Informática. Protección de Datos de Carácter Personal.*, 2° ed. (Madrid: Universidad Nacional de Educación a Distancia, UNED, 2003), pp. 76-78; Mónica ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa* (Valencia: Tirant lo Blanch, 2006), pp. 283-284; Lucrecio REBOLLO DELGADO, *Vida privada y protección de datos en la Unión Europea* (Madrid: Dykinson, 2008), pp. 120-133.

[496] Cfr. Artículo 1.1 del Reglamento 45/2001.

[497] Cfr. Artículo 1.2. del Reglamento 45/2001. El Supervisor Europeo de Protección de Datos (SEPD) es una autoridad de control independiente encargada de garantizar que las instituciones y los organismos de la UE cumplan sus obligaciones en materia de protección de datos, establecidas en el Reglamento (CE) nº 45/2001
relativo a la protección de datos. Los cometidos principales del SEPD son el control, la consulta y la cooperación. Las competencias de control del SEPD abarcan el tratamiento de los datos personales por las instituciones y los organismos de la UE, pero no incluyen el tratamiento de datos en los Estados Miembros. El SEPD también asesora a las instituciones y los organismos de la UE sobre todos los asuntos que repercutan en la protección de los datos personales. Cfr. http://www.europarl.europa.eu/ftu/pdf/es/FTU_4.12.8.pdf. [Consulta: 6.10.2013]..

[498] Artículo 3.1.

otros), todas ellas remiten al Reglamento 45/2001 como norma supletoria aplicable al tratamiento de datos personales, y al Supervisor Europeo de Protección de datos como autoridad de control.

CAPÍTULO SEXTO

MARCO JURÍDICO DE LA PROTECCIÓN DE DATOS EN EL ÁMBITO ESPECÍFICO DE LA COOPERACIÓN POLICIAL O CON INCIDENCIA EN ÉL

SUMARIO: INTRODUCCIÓN. 1. ANÁLISIS CRÍTICO DE LA DECISIÓN MARCO 2008/977/JAI, RELATIVA A LA PROTECCIÓN DE DATOS PERSONALES TRATADOS EN EL MARCO DE LA COOPERACIÓN POLICIAL Y JUDICIAL EN MATERIA PENAL; 1.1. Dificultades para su elaboración; 1.2. Objetivo declarado vs alcance real de la Decisión Marco; 1.3. Ámbito de aplicación limitado; 2. ANÁLISIS CRÍTICO DE LA PROPUESTA DE NUEVA DIRECTIVA QUE REEMPLAZA LA DECISIÓN MARCO 2008/977/JAI DEL CONSEJO; 2.1. Origen y configuración jurídica; 2.2. Objeto; 2.3. Ámbito de aplicación; 3. TRATADO DE PRÜM Y SU INCORPORACIÓN A LA NORMATIVA EUROPEA POR MEDIO DE LA DECISIÓN 2008/615/JAI; 3.1. Aspectos generales; 3.2. Objeto y ámbito de aplicación; 3.3. Nivel de protección otorgado a los datos personales; 4. INSTITUCIONES COMUNITARIAS DE COOPERACIÓN POLICIAL Y JUDICIAL CON DISPOSICIONES PARTICULARES SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL; 4.1. La Oficina Europea de Policía (Europol); 4.2. La Unidad de Cooperación Judicial (Eurojust); 4.3. Agencia Europea para la gestión de la cooperación operativa en las fronteras exteriores de los Estados Miembros de la Unión Europea (Frontex); 5. SISTEMAS INFORMÁTICOS DE GRAN MAGNITUD EN EL ESPACIO DE JUSTICIA, LIBERTAD Y SEGURIDAD; 5.1. El Sistema de Información Schengen (SIS); 5.2. El Sistema de Información de Visados (SIV); 5.3. El Sistema de Comparación de Huellas Dactilares (Eurodac).

INTRODUCCIÓN

El actual marco normativo europeo sobre protección de datos en el ámbito de la cooperación policial penal carece de un desarrollo coordinado y homogéneo, y se presenta como un conjunto atomizado por áreas específicas. Ello se debe a diversos factores. En primer lugar, a la inexistencia, hasta hace poco, de una norma de carácter general destinada a regular la materia, rol que debió cumplir la Decisión Marco 2008/977/JAI, pero que, atendido su limitado ámbito de aplicación, no cumplió, situación que ahora se intenta superar mediante la creación de una nueva Directiva Europa.[499] En segundo lugar, ha influido el hecho de que cada norma desarrollada antes

[499] COM (2012) 10 final, Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las

de la Decisión Marco 2008, referida al tratamiento de datos personales con fines de prevención y represión penal, consagró disposiciones particulares, que en su mayoría se remitía al derecho interno de cada Estado como forma o mecanismo de resguardar los derechos de los titulares de los datos, generando una disparidad de criterios de un Estado a otro. Ante la variedad de normativa existente en la materia en el ámbito de la Unión Europea, el bloque normativo constituido por el Convenio 108 de 1981, su Protocolo adicional de 2001 y la Recomendación (87) 15, todas del Consejo de Europa, pasaron a constituir en el estándar mínimo de protección a respetar por parte de los Estados y organismo comunitarios en el tratamiento de los datos personales, en el ámbito específico de la cooperación policial y judicial en materia penal.

A todo lo anterior se suman algunas iniciativas llevadas a cabo en el seno de la Unión Europea, como el desarrollo del Programa de La Haya, la incorporación de los aspectos esenciales del Tratado de Prüm en el ordenamiento jurídico de la Unión Europea a través de la Decisión 2008/615/JAI del Consejo, de 23 de junio, o el desarrollo del llamado PNR europeo, a través de la propuesta de Decisión Marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros con fines represivos. Todo ello pone de manifiesto la voluntad del legislador europeo de avanzar en el intercambio de información con finalidades de investigación y lucha contra la delincuencia y el terrorismo, pero por otra parte generan dudas en relación con la protección de derechos fundamentales en general y la protección de datos personales en particular. Dudas que surgen, en parte, de la indefinición de un marco jurídico comunitario claro y efectivo de protección de datos en el ámbito del viejo tercer pilar ahora comunitarizado.[500] Atendido lo anterior, cobra importancia analizar si la nueva Propuesta de Directiva que pretende derogar y reemplazar a la Decisión Marco 2008/977/JAI se hace cargo de todos los problemas que se suscitan con la aplicación de normas de protección de datos en el ámbito específico de la prevención y represión penal.

---

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. Bruselas, 25.1.2012.

[500] Cristina DIETRICH PLAZA, «Las tensiones entre libertad y seguridad en el marco jurídico actual de protección de datos de carácter personal en la Unión Europea», op. cit., pp. 185-186.

También revisaremos algunos acuerdos o tratados internacionales suscritos por algunos miembros de la Unión, sobre cooperación transfronteriza en el combate a la delincuencia, que ha terminado por incorporarse al acervo europeo. Por último, veremos el impacto que ha tenido en el derecho a la protección de datos personales de los principales sistemas de información que se han generado para mejorar la tarea de las instituciones europeas encargas del control y represión penal.

1. ANÁLISIS CRÍTICO DE LA DECISIÓN MARCO 2008/977/JAI, RELATIVA A LA PROTECCIÓN DE DATOS PERSONALES TRATADOS EN EL MARCO DE LA COOPERACIÓN POLICIAL Y JUDICIAL EN MATERIA PENAL

1.1. Dificultades para su elaboración

La necesidad de contar con una Decisión Marco sobre protección de datos en el ámbito de cooperación policial y judicial en materia penal, es un tema que estuvo presente en la Unión Europea, por lo menos, diez años antes de la aprobación de la Decisión Marco 2008/977/JAI de 27 de noviembre de 2008. En efecto, el año 1998 Italia presentó una iniciativa para debatir sobre la protección de datos personales en lo que en ese entonces constituía el tercer pilar comunitario.[501] En aquel momento el Consejo de Justicia y Asuntos de Interior adoptó el denominado Plan de acción de Viena.[502] Este establecía que en el contexto de la cooperación policial y judicial en materia penal, debían estudiarse las posibilidades de armonizar las normas sobre protección de datos en un plazo de dos años a partir de la entrada en vigor del Tratado de Ámsterdam. Sin embargo, en 2001 no pudo adoptarse un proyecto de Resolución relativa a las normas sobre protección de datos personales en los instrumentos del tercer pilar de la Unión Europea.[503] Luego, en junio de 2003, la Presidencia griega propuso un conjunto de principios generales en relación con la protección de datos personales en el marco del tercer pilar que se inspiraban en la Directiva 95/46/CE sobre protección de

[501] Cfr. Documento de trabajo del Consejo 8321/98JAI 15.

[502] Cfr. El Plan de acción del Consejo y de la Comisión sobre la mejor manera de *aplicar* las disposiciones del Tratado de Ámsterdam relativas a la creación de un espacio de libertad, seguridad y justicia. Texto adoptado por el Consejo Justicia y Asuntos de Interior de 3 de diciembre de 1998. Publicado en el DOUE nº C 19 de 23 de enero de 1999.

[503] Al respecto véase el Documento de trabajo del Consejo 6316 /2/01 REV 2 JAI 13.

datos y en la Carta de los Derechos Fundamentales de la Unión Europea.[504] En estas circunstancia llegamos a la propuesta de Decisión Marco del Consejo de 2005[505], que se concretó, luego de un largo proceso de elaboración, en la Decisión Marco 2008/977/JAI del Consejo.

La Decisión Marco 2008/977/JAI, tuvo un extenso proceso de elaboración. Su inicio se puede fechar el 4 de octubre de 2005, con la presentación de la propuesta de Decisión Marco formulada por la Comisión[506], y su término con la adopción de la misma, ocurrida el 27 de noviembre de 2008, es decir, habiendo transcurrido más de tres años. En este periodo podemos constatar que en un inicio la propuesta contó con el apoyo del conjunto de actores involucrados, atendida la necesidad de una norma vinculante para todos los Estados Miembros de la Unión en el antiguo tercer pilar comunitario. No obstante, a poco andar, el camino se transformó en escabroso con dictámenes muy críticos, por parte del Parlamento y del Supervisor Europeo de Protección de Datos, sobre muchos aspectos contenidos en el proyecto de Decisión Marco.

En efecto, presentada y conocida la propuesta en su cabalidad, tanto el Parlamento Europeo[507] como de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior[508], emitieron informes donde se sugieren diversas modificaciones y enmiendas al texto presentado por el Consejo. Entre ellas destacan: que la Unión Europea debería asegurar el mismo nivel de protección de los datos personales no sólo a los ciudadanos europeos, sino también a los ciudadanos de cualquier tercer país; que en el intercambio de datos con terceros países deben respetar dos principios fundamentales, esto es, asegurarse que los datos sólo se transfieran a terceros países que garanticen un nivel adecuado de protección de datos y que los datos que se reciban de terceros países

[504] Véase la 2514ª Reunión del Consejo, Justicia y Asuntos de Interior, realizada en Luxemburgo, los días 5 y 6 de junio de 2003; y el documento del Consejo 9845 /03 (Presse 150), p. 32.
[505] Cfr. Propuesta de Decisión Marco del Consejo, 2005/0202 (CNS), relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, de 4.10.2005. SEC (2005) 1241.
[506] Ídem.
[507] Cfr. Informe Final del Parlamento Europeo nº A6-0192/2006, de fecha 18 de mayo de 2006, sobre la propuesta de Directiva marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.
[508] Cfr. Informe (A6-0192/2006) de la Comisión de Libertades civiles, Justicia y Asunto de interior, *http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+ADDON+A6-2006-0192+ERR-01-ES+DOC+PDF+V0//ES* [fecha consulta: 18 de junio de 2010]

respeten los derechos fundamentales. Respecto de la gestión de los datos a cargo de particulares, especialmente en el marco de asociaciones entre los sectores público y privado, señala que estos últimos estarán sometidos, como mínimo, a las mismas condiciones en materia de seguridad de datos que las previstas para las autoridades públicas competentes. Asimismo, señala que es conveniente añadir una referencia al Sistema de Información de Visado (SIV), para que la presente Decisión Marco se aplique también al acceso por parte de los servicios represivos al sistema. Del mismo modo, señala que es indispensable introducir los principios de finalidad y proporcionalidad como criterios para establecer la licitud del tratamiento de datos. Respecto del tratamiento de datos sensibles, el informe planteababa que sólo debería autorizarse en la medida en que el tratamiento se realice en interés de esta persona. En el mismo sentido, señalaba que la negativa a dar el consentimiento no debería tener efectos negativos para la persona afectada, y contenía una serie de enmiendas relacionadas con los datos sensibles, particularmente datos de ADN y biométricos.[509]

En el proceso de elaboración de la Decisión Marco, también intervinieron las Autoridades de Protección de Datos de los Estados Miembros de la Unión Europea[510] (en adelante indistintamente, APD) y el Supervisor Europeo de Protección de Datos (en adelante indistintamente, SEPD).[511] Tanto el SEPD como las APD, expresaron su firme apoyo a la idea de crear un nuevo instrumento jurídico para regular la protección de datos personales en el antiguo tercer pilar comunitario, con el objeto de garantizar el mismo nivel de protección de datos que el establecido para lo que correspondía al primer pilar comunitario. Pero una vez conocida la propuesta del Consejo, ambos organismo se mostraron muy críticos, entre otros temas, sobre su ámbito de aplicación;

[509] Cfr. *http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A6-2006 0192&language=ES#title1* [fecha de consulta: 18 de junio de 2013]. Luego de las enmiendas introducidas por el Parlamento Europeo, se dicta la Resolución legislativa del Parlamento Europeo, de fecha 27.6.2006 y, posteriormente, una nueva resolución legislativa del Parlamento Europeo de fecha 23.9.2008, sobre la última versión presentada de la propuesta de Decisión Marco . De la lectura de exposición de motivos, se puede concluir que en un inicio el Parlamento acoge favorablemente la propuesta de la Comisión, advirtiendo que, desde la creación del tercer pilar, el Parlamento viene solicitando normas de protección de datos en materia de cooperación judicial y policial que sean comparables a las normas vigentes en el Derecho comunitario. Estas normas deberían reemplazar, por consiguiente, los principios y derechos que figuran en el Convenio 108 y la Recomendación 87 del Consejo de Europa.

[510] Conferencia de las Autoridades Europeas de Protección de Datos, Budapest del 24 al 25 de abril de 2006.

[511] Los Dictámenes del SEPD, se pueden consultar en *http://www.edps.europa.eu/EDPSWEB/edps/EDPS*

la falta de limitación clara de finalidades y usos incompatibles; la calidad de los datos y la ausencia de un grupo de trabajo similar al del artículo 29 de la Directiva 96/46/CE.[512]

1.2. Objetivo declarado vs alcance real de la Decisión Marco

Si analizamos el contenido total de la Decisión Marco 2008/977/JAI, nos encontramos con que existe un objeto, o más bien, un objetivo declarado que contrasta con los alcances reales de la misma.[513] Desde una visión amplia, la Decisión Marco se encuadra dentro del objetivo general de la Unión de mantener y desarrollar un espacio de libertad, seguridad y justicia que ofrezca a sus ciudadanos respeto sus derechos y seguridad.[514] Para avanzar en este doble objetivo se propone mejorar la legislación en el ámbito del antiguo tercer pilar, que regulaba el título VI del Tratado de la Unión Europea —cooperación policial y judicial en materia penal— en cuanto a su eficacia y a su legitimidad, pero respetando de los derechos fundamentales, en particular el derecho a la intimidad y a la protección de los datos personales. La existencia de normas comunes para el tratamiento y la protección de los datos personales, tratados con el fin de prevenir y luchar contra la delincuencia, contribuyen a la consecución de ambos objetivos.[515] En esta línea el artículo 1.1. de la Decisión Marco 2008/977/JAI señala que su objetivo es «garantizar un alto nivel de protección de los derechos y libertades fundamentales de las personas físicas y en particular su derecho a la intimidad en lo que respecta al tratamiento de datos personales en el marco de la cooperación policial y judicial en materia penal, contemplada en el título VI del Tratado de la Unión Europea, garantizando al mismo tiempo un alto nivel de seguridad pública». Por tanto, el objetivo de la norma en estudio sería el establecimiento de normas comunes para la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.[516]

[512] El artículo 29 de la Directiva 95/46/CE, crea un grupo de estudio de carácter consultivo e independiente, integrado por representantes de las autoridades creadas por los Estados Miembros, las instituciones y organismos comunitarios, y por un representante de la Comisión.
[513] Llama la atención que la Decisión Marco no señala expresamente su «objeto», esto es, su fin, y sólo se limita a señalar su «objetivo». Cfr. artículo 1.1. y considerandos 1, 3, 11 y 42 de la Decisión Marco.
[514] Cfr. Considerando 1 de la Decisión Marco.
[515] Cfr. Considerando 3 de la Decisión Marco.
[516] Cfr. Considerando 42 de la Decisión Marco.

Ahora bien, el objetivo perseguido por la Decisión Marco sólo se verifica parcialmente, toda vez que su campo de aplicación es sumamente reducido, lo que impide cumplir con el fin de establecer un alto nivel de protección en todos los ámbitos del tratamiento de datos personales realizados en materia de cooperación policial y judicial europea, como pasamos a detallar en el siguiente apartado.

1.3. Ámbito de aplicación limitado

Uno de los puntos más criticados a la Decisión Marco 2008/977/JAI es su limitado ámbito de aplicación, ya que sólo rige el tratamiento de los datos personales transmitidos o puestos a disposición entre Estados Miembros.[517] Los supuestos concretos para la aplicabilidad de la norma se restringen a tres: que los Estados Miembros transmitan o pongan a disposición entre sí datos personales[518]; que los Estados Miembros transmitan a autoridades o sistemas de información creados en virtud del título VI del Tratado de la Unión Europea (antiguo tercer pilar), o pongan a su disposición datos personales[519]; y que las autoridades o sistemas de información creados en virtud del Tratado de la Unión Europea o del Tratado constitutivo de la Comunidad Europea transmitan a las autoridades competentes de los Estados Miembros, o pongan a su disposición datos personales.[520] Tanto la transmisión como la recepción de los datos efectuada para los fines señalados, quedan sujetos a las prescripciones de la Decisión Marco para su ulterior tratamiento. Por último, hay que tener presente que cuando se habla de autoridades o sistemas de información de la Unión Europea, ellas se refieren a las del antiguo tercer pilar[521], ya que las autoridades o sistemas de información del antiguo primer pilar se contemplan sólo como remitentes.[522]

En cuanto al tipo de soporte en que se realiza dicho tratamiento, la Decisión Marco 2008/977/JAI se aplica «tanto al tratamiento automatizado como no automatizado, ya sea total o parcial, de datos personales que formen parte o esté

[517] Cfr. Considerando 7 de la Decisión Marco .
[518] Artículo 1.2.a)
[519] Artículo 1.2 b)
[520] Artículo 1.2 c)
[521] Por ejemplo EUROPOL, EUROJUST, OLAF.
[522] Por ejemplo EURODAC, SIS, VIS, SIA. En el mismo sentido, véase BAYO DELGADO, «La cooperación policial internacional a la luz de la Propuesta revisada de Decisión Marco relativa a la protección de datos», p. 29.

previsto que vayan a formar parte de un fichero».[523] En consecuencia, sus disposiciones rigen para todo tipo de tratamiento, en cualquier tipo de soporte. El hecho de incluir el tratamiento manual, constituye un avance respecto de lo dispuesto en el Convenio 108 y la Recomendación 87(15) del Consejo de Europa[524], que sólo se aplican al tratamiento automatizado de datos, y lo acerca más al criterio de la Directiva 95/46/CE, que también contempla ambos tipos de tratamiento. También debe tomarse en cuanta que sus disposiciones sólo se aplican respecto de datos personales de las personas físicas, por lo que quedan descartados los tratamientos de datos de las personas jurídicas o morales. En cuanto a los ficheros, este comprende a todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.[525]

Por otra parte, entre las materias que la Decisión Marco excluye de su ámbito de aplicación material encontramos, en primer lugar, el tratamiento «doméstico» de datos policiales y judiciales en materia penal, esto es, a los datos personales que un Estado Miembro haya obtenido en el ámbito de aplicación de la presente Decisión Marco y que tengan su origen en ese mismo Estado miembro.[526] Por tanto, quedan excluidos todos los tratamientos de datos efectuados a nivel interno, vinculados a la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales como la ejecución de sanciones penales.[527] Este ha sido uno de los puntos más criticados por el Supervisor Europeo de Protección de Datos y las Autoridades de Protección de Datos de los Estados Miembros de la Unión Europea, ya que abre la posibilidad de un doble régimen en el tratamiento de este tipo de datos, uno interno o doméstico y otro para los supuestos contemplados en la Decisión Marco.[528]

---

[523] Artículo 1.3

[524] Cabe tener presente que la Recomendación 87(15) del Consejo de Europa, permite a los Estado miembro "ampliar" los principios contenidos en ella a los datos no tratados de forma automatizada.

[525] Artículo 2. d)

[526] Cfr. Considerando 9, de la Decisión Marco 2008/977/JAI.

[527] Para reforzar esta idea, la Decisión señala en sus considerandos que «de esta limitación no deben extraerse conclusiones relativas a la competencia de la Unión para adoptar actos relativos a la recopilación y tratamiento de datos personales en el ámbito nacional ni a la conveniencia de que la Unión tenga dicha competencia en el futuro». Cfr. Considerando 7, segunda parte, de la Decisión Marco 2008/977/JAI.

[528] Sobre las críticas al ámbito de aplicación de la Decisión Marco , véase Joaquín BAYO DELGADO, «La cooperación policial internacional a la luz de la Propuesta revisada de Decisión Marco relativa a la protección de datos», en *La protección de datos en la cooperación policial y judicial* (Pamplona: Aranzadi, 2008), pp. 29-30; Cristina DIETRICH PLAZA, «Las tensiones entre libertad y seguridad en el marco jurídico actual de protección de datos de carácter personal en la Unión Europea», en *Libertad,*

La Decisión Marco 2008/977/JAI, tampoco afecta el tratamiento de datos personales realizado por la Oficina Europea de Policía (Europol), por la Unidad Europea de Cooperación Judicial (Eurojust), el Sistema de Información de Schengen (SIS) y el Sistema de Información Aduanero (SIA), ni en general, a los que permiten a las autoridades acceder directamente a determinados sistemas de datos de otros Estados miembros, que tengan un objeto diferente al señalado en esta DM 2008/977/JAI.[529] Tampoco se aplica la Decisión Marco a las disposiciones de protección de datos que rigen la transferencia automatizada de perfiles de ADN, datos dactiloscópicos y datos de los registros nacionales de matriculación de vehículos, en virtud de la Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza.[530] Asimismo, la Decisión Marco excluye específicamente de su ámbito de aplicación las materias propias del antiguo segundo pilar comunitario, estos es, las vinculadas a los intereses esenciales de seguridad del Estado y a las actividades específicas de inteligencia en éste sector.[531]

El legislador comunitario justifica las exclusiones señaladas anteriormente, atendiendo a un supuesto principio de especialidad de dichas normas. Se señala que estos sistemas de información (Europol, Eurojust, SIS y VIS) «contienen un conjunto completo y coherente de normas que abarcan todos los aspectos correspondientes de la protección de los datos (principios de calidad, normas sobre seguridad de los datos, reglamentación de los derechos y protecciones de los interesados, organización del control y responsabilidad), que reglamentan estos asuntos con más detalle que la presente Decisión Marco».[532] Por tanto, se privilegia la aplicación de dichas normas por sobre la protección contenida en la Decisión Marco. Creemos que lo anterior solo se podría justificar en la medida que las previsiones sobre protección de datos contenidas en las citadas bases de datos, contengan efectivamente disposiciones que garanticen un

seguridad y transformaciones del Estado, ed. Joan Lluís PÉREZ FRANCESCH (Barcelona: Institut de Ciències Polítiques i Socials, 2009), pp. 194-195.

[529] Cfr. Considerando 39 de la Decisión Marco .

[530] Ídem. Cabe recordar que la Decisión 2008/615, es el instrumento normativo que transpuso al ordenamiento jurídico europeo el Tratado de Prüm. Al respecto véase *infra* apartado 3 del capítulo sexto de este trabajo.

[531] Cfr. Artículo 1.4 de la Decisión Marco .

[532] Considerando 39, de la Decisión Marco 2008/977/JAI.

nivel igual o mayor de protección que la Decisión Marco, lo que obligatoriamente nos obliga a realizar una comparación del nivel de protección de cada uno de ellos.

Al respecto cabe recordar que 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[533], no se aplica al tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del derecho comunitario, como son las contempladas en el título VI del Tratado de la Unión Europea, ni en ningún caso a las operaciones de tratamiento de datos relacionadas con la seguridad pública, la defensa, la seguridad del Estado o las actuaciones del Estado en materia penal.[534] Ante la ausencia de un instrumento normativo equivalente a la Directiva 95/46/CE en el ámbito de la cooperación judicial y policial en materia penal, los cuerpos normativos que regularon materias vinculadas al ámbito de cooperación judicial y policial, se vieron obligados a recurrir al Convenio 108 del Consejo de Europa de 1981, su Protocolo Adicional y a la Recomendación 15(87) del Comité de Ministros a los Estados, que regula el uso de datos personales en el sector de la policía.[535] Ahora bien, producto del limitado ámbito de aplicación de la Decisión Marco 2008/977/JAI, el bloque de garantía mínimas a respetar, en el ámbito del antiguo tercer pilar comunitario, seguiría dado por estos tres cuerpos normativos del Consejo de Europa.[536]

Como se pude apreciar, el ámbito de aplicación de la Decisión Marco, es sumamente restringido, ya que sus disposiciones no se aplican a todos los tratamientos ni a todas las fases del tratamiento de datos personales en el ámbito de la cooperación judicial y policial en materia penal. Su aplicabilidad se limita sólo a las transferencias de datos entre Estados Miembros y entre éstos y ciertos sistemas de información

[533] Directiva 95/46/CE del Parlamento Europeo y Consejo de la Unión Europea, de 24 de octubre de 1995, relativa a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, publicada en el DOCE L 281, de 23 de noviembre de 1995.
[534] Cfr. los considerandos 13, 16 y el artículo 3 de la Directiva 95/46/CE.
[535] También como forma paliativa a esta ausencia de regulación, se optó por incluir ciertos principios y derechos sobre protección de datos en los propios textos normativos, como ocurrió en la Decisión 2008/615/JAI, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza. En el mismo sentido, véase DIETRICH PLAZA, «Las tensiones entre libertad y seguridad en el marco jurídico actual de protección de datos de carácter personal en la Unión Europea», p. 209.
[536] Cfr. Considerando 20 de la Decisión 2008/615/JAI.

comunitarios. En consecuencia, la Decisión Marco no puede equipararse a la Directiva 95/46/CE respecto del antiguo primer pilar comunitario, que regula tanto el tratamiento realizado en los Estados Miembros como las transferencias realizadas a terceros Estados dentro y fuera de la Unión. Asimismo, la Directiva de 1995 regula el **ciclo vital del dato personal** en su integridad, es decir, desde la fase de captación o elaboración, hasta su cancelación o eliminación final.

Con el contenido actual de la Decisión Marco, se perdió una oportunidad de homogeneizar la regulación del tratamiento de los datos personales en todos los Estados de la Unión, exigiendo estándares comunes de protección para los datos personales tratados en el ámbito de la cooperación policial y judicial. Por último, lo que más nos preocupa, es que la nueva propuesta de Directiva que pretende derogar y sustituir a la Decisión Marco 2008/977/JAI, reproduce gran parte de los problemas planteados, ya que excluye también de su ámbito de aplicación los tratamientos realizados por los organismos de la Unión encargados precisamente de la cooperación judicial y policial (Europol y Eurojust), y sólo avanza en cuanto incorporar el tratamiento nacional de los datos policiales.

2. ANÁLISIS CRÍTICO DE LA PROPUESTA DE NUEVA DIRECTIVA QUE REEMPLAZA LA DECISIÓN MARCO 2008/977/JAI DEL CONSEJO

2.1. Origen y configuración jurídica

La propuesta de Directiva del Parlamento Europeo y del Consejo, de 25 de enero de 2012, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos (en adelante, la Propuesta de Directiva)[537], responde, por una parte, a la necesidad de adecuar el marco jurídico de la

[537] COM (2012) 10 final. En este apartado sólo revisaremos los aspectos generales de la Propuesta de Directiva, reservando su análisis en profundidad para el estudio particularizado del tratamiento de datos personales en el ámbito de la prevención y represión penal, tratado en los capítulos séptimo y octavo de esta investigación.

protección de datos personales en la UE a lo prescrito por el Tratado de Lisboa[538] y, por otra, a tratar de corregir importantes falencias que posee la Decisión Marco 2008/977/JAI, norma que sería reemplazada y derogada por la propuesta de Directiva en estudio.

La propuesta tiene como base jurídica específica el artículo 16, apartado 2 del TFUE, que es una nueva base jurídica introducida por el Tratado de Lisboa para la adopción de normas relativas a la protección de las personas físicas con respecto al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos, y por los Estados Miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión. Con la nueva propuesta de Directiva se da cumplimiento a lo prescrito por el mismos artículo 16 del TFUE, que obliga al legislador europeo a establecer normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales en todos los ámbitos, incluido la cooperación judicial en materia penal y la cooperación policial. Ahora bien, dada la naturaleza específica del ámbito de la cooperación policial y judicial en materia penal, se reconoció explícitamente en una Declaración aneja al Tratado[539] que se podrían requerir normas específicas para el antiguo tercer pilar comunitario. En esta línea, la propuesta de Directiva se presenta como un intento de homogenizar los niveles de protección que se brindan en los otros ámbitos del derecho de la Unión (particularmente el antiguo primer pilar), pero teniendo en consideración las necesidades específicas en el ámbito de la cooperación policial y judicial, que en la práctica se traduce en una serie de limitaciones y excepciones al ejercicio de los derechos de los titulares de los datos.

Es importante destacar también, dentro de los aspectos generales de la propuesta de Directiva, el esfuerzo realizado por darle una mayor legitimidad democrática al proceso de elaboración de la misma. Con dicho fin se consultó a todas las partes interesadas (operadores y conocedores del sistema)[540], así como también a los

[538] Cfr. COM (2012) 9 final. Este nuevo marco jurídico, estaría dado por la *propuesta de Reglamento general* de protección de datos y por la *propuesta de Directiva* en estudio. Sobre las modificaciones que trae el Tratado de Lisboa en relación al derecho fundamental de la protección de datos, véase *supra* apartado 1 del capítulo quinto de este trabajo.
[539] Declaración n° 2 aneja al Tratado de Lisboa.
[540] La consulta con todas las partes interesadas sobre la revisión del actual marco jurídico para la protección de datos de carácter personal, incluyó dos fases: la primera se realizó entre el 9 de julio y el 31

ciudadanos europeos.[541] También se tuvieron a la vista varios estudios[542] y Dictámenes, tanto del GT29[543] como del Supervisor Europeo de Protección de Datos[544], y un estudio de impacto de las distintas opciones planteadas.[545] Estas propuestas de reformas han contado con el apoyo político del Parlamento Europeo, el Consejo de la Unión Europea y el Comité Económico y Social Europeo.[546]

Para la elaboración de la propuesta de Directiva se realizó, por parte de la Comisión, una evaluación de impacto de las diversas opciones de actuación.[547] La evaluación de impacto se basó en tres objetivos estratégicos: mejorar la dimensión del mercado interior de la protección de datos, hacer más efectivo el ejercicio de los derechos de protección de datos por los ciudadanos y crear un marco global y coherente que abarque todos los ámbitos de competencia de la Unión, incluida la cooperación

---

de diciembre de 2009, y se denominó precisamente *Consulta sobre el marco jurídico para el derecho fundamental a la protección de datos de carácter personal*. La Comisión recibió 168 respuestas, 127 de personas físicas, organizaciones y asociaciones empresariales, y 12 de autoridades públicas. La segunda fase, se desarrolló del 4 de noviembre de 2010 al 15 de enero de 2011, *Consulta sobre el enfoque global de la Comisión sobre la protección de datos de carácter personal en la Unión Europea*. En esta etapa, la Comisión recibió 305 respuestas, de las cuales 54 procedían de ciudadanos, 31 de autoridades públicas y 220 de organizaciones privadas, especialmente de asociaciones empresariales y organizaciones no gubernamentales. Las respuestas no confidenciales pueden consultarse en el sitio internet de la Comisión: http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm. y http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm. [Consultado el 08.08.2013]

[541] Eurobarómetro espacial (EB) 359, *Protección de datos e identidad electrónica en la UE*, realizado entre noviembre y diciembre de 2010. Publicado en 2011 y disponible en http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

[542] Véase el estudio sobre las ventajas económicas de las tecnologías potenciadoras de la privacidad y el estudio comparativo de los distintos enfoques ante los nuevos retos en materia de protección de la privacidad, en particular a la luz de los avances tecnológicos, de enero de 2010. Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf

[543] Sus Dictámenes se pueden consultar en http://ec.europa.eu/justice/protección de datos/article-29/documentation/index_en.htm..

[544] Sus Dictámenes están disponibles en el sitio internet del SEPD: http://www.edps.europa.eu/EDPSWEB/. Sobre el Supervisor Europeo de Protección de Datos, véase el capítulo X.X de este trabajo.

[545] Véase el Dictamen emitido por Comité de Evaluación de Impacto (CEI), de 9 de septiembre de 2011.A raíz del dictamen del CEI, se aclararon los objetivos del marco jurídico en vigor; en la sección consagrada a la definición de problemas se añadieron más elementos de prueba y explicaciones/aclaraciones adicionales.

[546] Cfr. Resolución del Parlamento Europeo, de 6 de julio de 2011, «sobre un enfoque global de la protección de los datos personales en la Unión Europea», (2011/2025(INI); Las Conclusiones del Consejo de la Unión Europea, de 24 de febrero de 2011, en las que respalda en términos generales la intención de la Comisión de reformar el marco de la protección de datos; y CESE 999/2011.

[547] Cfr. Comisión Europea «Estudio de Evaluación de Impacto sobre Reglamento del Parlamento Europeo y del Consejo relativa a la protección de los las personas con respecto al tratamiento de datos personales ya la libre circulación de estos datos (Reglamento general de protección de datos) y Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas en lo que respecta al tratamiento de datos personales por las autoridades competentes para los fines de prevención, investigación, detección o enjuiciamiento de delitos o la ejecución de sanciones penales, y la libre circulación de estos datos», SEC (2012) 72.

policial y judicial en materia penal.[548] Respecto a este último objetivo en particular, se evaluaron varias opciones estratégicas: la primera, que básicamente ampliaba el ámbito de aplicación de las normas de protección de datos en este campo y abordaba las carencias y otras cuestiones planteadas por la Decisión Marco; una segunda de mayor alcance, con normas muy prescriptivas y estrictas, que también entrañaba la modificación inmediata de todos los demás instrumentos del «antiguo tercer pilar»;[549] y una tercera opción «minimalista», basada en gran medida en comunicaciones interpretativas y en medidas de apoyo político, tales como programas de financiación y herramientas técnicas, con una mínima intervención legislativa, la que finalmente no se consideró apropiada para tratar las cuestiones señaladas en este ámbito en relación con la protección de datos.[550] La opción elegida, representa una posición intermedia o punto de equilibrio, ya que amplía el ámbito de aplicación de la normativa al tratamiento nacional o doméstico y otras críticas formuladas a la Decisión Marco, pero se pierde la oportunidad de establecer criterios comunes en el tratamiento de datos personales con fines de prevención y represión penal de todos los operadores jurídicos, ya que deja subsistente los regímenes jurídicos de los SIS, VIS, Europol, entre otros. De la opción tomada, queda claro que la voluntad de avanzar en la materia, pero a un ritmo pausado; en otros términos, no existe aún la voluntad política para un cambio más radical al sistema de protección de datos en éste ámbito, por lo que tendremos que esperar, si se llega aprobar, una próxima revisión de la aplicación de este nuevo marco normativo para ver si toma la decisión política de realizar los cambios necesarios que precisa la defensa del derecho fundamental a la protección de datos personales en todos los ámbitos de la prevención y represión penal.

La propuesta de Directiva deroga y reemplaza a la Decisión Marco 2008/977/JAI, haciéndose cargo de algunas de las principales críticas que se han formulado a esta norma. Entre éstas desatacan su limitado ámbito de aplicación, ya que la Decisión Marco sólo se aplica al tratamiento transfronterizo de datos (dentro de la Unión), excluyendo las actividades de tratamiento por parte de las autoridades policiales y judiciales a nivel puramente nacional (tratamiento doméstico). Además, por su naturaleza y contenido, la Decisión Marco deja un amplio margen de maniobra a los

[548] Cfr. Propuesta Directiva COM (2012) 10 final, p. 4.
[549] Ídem.
[550] Ídem.

Estados Miembros para transponer sus disposiciones de Derecho interno, lo que puede provocar una disparidad de criterios en la aplicación y garantía concreta que se brinda a los ciudadanos en los diferentes Estados. Por último, también se critica que la Decisión Marco 2008/977 no contiene ningún mecanismo o grupo consultivo similar al Grupo del artículo 29 que sustente una interpretación común de sus disposiciones, ni establece competencias de ejecución de la Comisión, a fin de garantizar un enfoque común en su aplicación.[551]

2.2. Objeto

El objeto de la propuesta de Directiva es establecer normas relativas al tratamiento de datos personales con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.[552] Con ello se pretende lograr un doble objetivo: por una parte, proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales y, por otra, garantizar un alto nivel de seguridad pública, asegurando el intercambio de datos personales entre las autoridades competentes dentro de la Unión.[553]

Como se puede apreciar, la propuesta se alinea, por una parte, con la finalidad propia de todas las Directivas que se han dictado en materia de protección de datos desde la Directiva 95/46/CE, esto es, la protección de los derechos y libertades fundamentales y, en particular, de los datos personales (intimidad, vida privada).[554] Por otro lado, persigue reforzar la confianza mutua entre las autoridades policiales y judiciales de los distintos Estados Miembros, facilitando de esta forma la libre circulación de datos y la cooperación entre las autoridades policiales y judiciales.[555] En

[551] En cuanto a la ejecución de la Directiva por parte de los Estados Miembros, véase el Informe de la Comisión, basado en el artículo 29, apartado 2, de la DM 2008/977/JAI. Las conclusiones de dicho informe, se basan en las aportaciones realizadas por los Estados Miembros. Cfr. COM (2012) 12.
[552] Cfr. Artículo 1.1 de la propuesta de Directiva.
[553] Cfr. Artículo 1.2 de la propuesta de Directiva.
[554] Sobre este punto, cabe recordar que la nomenclatura utilizada varía esencialmente antes y después de la proclamación de la Carta Europea de Derechos Humanos, que reconoce explicita y autónomamente el derecho fundamental a la protección de datos personales en su artículo 8. Antes de ella, la referencia a ésta ámbito específico de protección se realizaban indistintamente a la intimidad y la vida privada.
[555] Al respecto la propuesta de Directiva, señala que «Asegurar un nivel uniforme y elevado de protección de los datos personales de las personas físicas y facilitar el intercambio de datos personales entre las autoridades competentes de los Estados Miembros es esencial para garantizar la eficacia de la

resumen, con la propuesta de Directiva se garantizaría que el derecho fundamental a la protección de datos de carácter personal se aplique de forma coherente en el contexto de todas las políticas (ámbitos) de la UE, contribuyendo con ello a facilitar la cooperación en el ámbito de la lucha contra la delincuencia en Europa.[556]

2.3. Ámbito de aplicación

El ámbito de aplicación de la propuesta de Directiva está señalado en su artículo 2, en los siguientes términos: «1. La presente Directiva se aplica al tratamiento de datos personales por parte de las autoridades competentes a los fines mencionados en el artículo 1, apartado 1.- 2. La presente Directiva se aplicará al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. 3. La presente Directiva no se aplicará al tratamiento de datos personales: a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión, en particular en lo que respecta a la seguridad nacional; b) por parte de las instituciones, órganos u organismos de la Unión».

Por tanto, sus disposiciones se aplican al tratamiento de datos personales realizados por las autoridades policiales y judiciales competentes, tanto a nivel transfronterizo como nacional. Se entiende por «autoridad competente» toda autoridad pública competente para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales.[557] La inclusión del

---

cooperación judicial en materia penal y de la cooperación policial. A tal efecto, el nivel de protección de los derechos y libertades de las personas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, debe ser equivalente en todos los Estados Miembros. La protección efectiva de los datos personales en la Unión no solo requiere la consolidación de los derechos de los interesados y de las obligaciones de quienes tratan dichos datos personales, sino también poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos personales en los Estados Miembros». Cfr. Considerando 7 de la Propuesta de Directiva.

[556] En este sentido el Plan de acción por el que se aplica el programa de Estocolmo, señala que «La Unión debe garantizar la aplicación coherente del derecho fundamental a la protección de datos. Debemos reforzar la posición de la UE en cuanto a la protección de los datos personales en el contexto de todas las políticas de la UE, incluida la represión policial y la prevención de la delincuencia, así como en nuestras relaciones internacionales». Cfr. COM (2010) 171 final, y la Comunicación de la Comisión Europea «Un enfoque global de la protección de los datos personales en la Unión Europea», COM (2010) 609 final de 4 de noviembre de 2010.

[557] Artículo 3.14 de la Propuesta de Directiva.

«tratamiento nacional» (doméstico), no está explícitamente señalado en el articulado de la Directiva, pero se deduce del conjunto de sus disposiciones, así como también de su exposición de motivos y considerandos.[558] Este punto constituye un avance en relación a la Decisión Marco 2008/977/JAI, la cual sólo tenía como ámbito de aplicación el tratamiento transfronterizo, pero es un avance limitado atendido al conjunto de restricción que se le colocan a la propuesta en cuanto a su extensión.

En efecto, la propuesta excluye de su ámbito de aplicación los tratamientos realizados en el ejercicio de una actividad que no esté comprendida en el ámbito de aplicación del Derecho de la Unión, en especial en lo referido a la seguridad nacional, ni a las operaciones de tratamiento efectuadas por instituciones, órganos y organismos de la Unión, que están sujetas al Reglamento (CE) nº 45/2001 y otras normas específicas.[559] De esta forma, y reincidiendo uno de los aspectos criticados a la Decisión Marco 2008/977/JAI, la propuesta de Directiva excluiría de su ámbito de aplicación el tratamiento de datos personales realizado por la Oficina Europea de Policía (Europol), por la Unidad Europea de Cooperación Judicial (Eurojust), el Sistema de Información de Schengen (SIS) y el Sistema de Información Aduanero (SIA). Tampoco se aplicaría la propuesta de Directiva a las disposiciones de protección de datos que rigen la transferencia automatizada de perfiles de ADN, datos dactiloscópicos y datos de los registros nacionales de matriculación de vehículos, en virtud de la Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008 sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza.[560] Asimismo, la propuesta de Directiva excluye

[558] Llama la atención que no se haya declarado explícitamente que la propuesta de Directiva sí abarca el tratamiento nacional o doméstico de los datos personales realizados por las policías y tribunales de los Estados Miembros. De hecho, trata el punto como una crítica a la normativa que se pretende derogar, señalando que «La Decisión Marco 2008/977/JAI tiene un ámbito de aplicación limitado, ya que solo se aplica al tratamiento transfronterizo de datos y no a las actividades de tratamiento por parte de las autoridades policiales y judiciales a nivel puramente nacional. Ello puede crear dificultades a las autoridades policiales y otras autoridades competentes en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial. No son siempre capaces de distinguir fácilmente entre el tratamiento meramente nacional y el transfronterizo no de prever si determinados datos personales pueden convertirse en objeto de un intercambio transfronterizo en una fase posterior». Cfr. Propuesta de Directiva COM (2012) 10 final, pp. 2, 7, 16, 56 y 57.

[559] Cfr. Artículo 2.3 de la propuesta de Directiva.

[560] Al respecto, el artículo 59 de la propuesta de Directiva, señala: « Las disposiciones específicas relativas a la protección de datos personales en lo que respecta al tratamiento de datos personales por parte de autoridades competentes a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales en actos de la Unión adoptados antes de la fecha de adopción de la presente Directiva que regulen el tratamiento de datos personales entre los Estados Miembros y el acceso de autoridades designadas de los Estados Miembros a los sistemas de información

específicamente de su ámbito de aplicación las materias propias del antiguo segundo pilar comunitario, estos es, las vinculadas a los intereses esenciales de seguridad nacional de los Estados.[561]

El legislador comunitario no justifica en la propuesta de Directiva porque razón restringe tanto el ámbito de aplicación de la Directiva propuesta. Creemos que la respuesta la podemos encontrar en la Decisión Marco que se trata de reemplazar, ya que ambas aplican las mismas restricciones de aplicabilidad en relación a los sistemas de información (SIS, SIV, entre otros) y a los órganos comunitarios de cooperación policial y judicial (Europol y Eurojust). La Decisión Marco, señala que estos sistemas de información, en algunos casos, contienen un conjunto completo y coherente de normas que abarcan todos los aspectos correspondientes de la protección de los datos (principios de calidad de los datos, normas sobre seguridad de los datos, reglamentación de los derechos y protecciones de los interesados, organización del control y responsabilidad) que reglamentan estos asuntos con más detalle que la propia Decisión Marco.[562] Por tanto, atendiendo a un criterio de especificidad, se privilegiaría la aplicación de aquellas normas por sobre las disposiciones de la propuesta de Directiva, por constituir las primeras, supuestamente, un conjunto "complejo y coherente", cuya operatividad ya ha quedado supuestamente demostrada. Creemos que esta premisa sólo se puede justificar en la medida que las previsiones sobre protección de datos de dichas normas, contengan efectivamente disposiciones que garanticen un nivel igual o mayor de protección que la contenida en la Decisión Marco o en la propuesta de Directiva que la reemplaza. Lo contrario implicaría aceptar una rebaja en nivel de protección que se brinda a las personas, sin otra justificación que el hecho de que su regulación esté en una norma especial, lo que repugna al fin declarado en todos los instrumentos, en el sentido de garantizar y proteger efectivamente los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

---

establecidos con arreglo a lo dispuesto en los Tratados en el ámbito de la presente Directiva no se verán afectadas». Cabe recordar que la Decisión 2008/615, es el instrumento normativo que transpuso al ordenamiento jurídico europeo el Tratado de Prüm.

[561] De la lectura de la propuesta de Directiva, queda claro que la misma realiza una distinción entre «seguridad pública» y «seguridad nacional», refiriendo las primeras a las materias que antes serían propias del tercer pilar comunitario y, la segunda, a las materias propias del antiguo segundo pilar comunitario. Cfr. Considerandos 15, 33 y 49; y artículos 2.3.a), 7.d), 11.4 c) y d), 13.1. c) y d), 34, 36 de la propuesta de Directiva.

[562] Considerando 39, de la Decisión Marco 2008/977/JAI.

En definitiva, proponemos realizar un examen de ponderación respecto del nivel de protección de cada uno de los instrumentos normativos que contienen normas específicas sobre tratamiento de datos en el ámbito policial y judicial, en relación a las garantías contenidas en la DM 2008/977/JAI y la propuesta que pretende derogarla y sucederla.[563] Si de este examen de ponderación resulta que el cuerpo normativo particular disminuye los niveles de protección, se puede y debe recurrir a la aplicación supletoria de las disposiciones contenidas en los instrumentos normativos generales (Decisión Marco o propuesta de Directiva). Es más, creemos que en los futuros procesos de reforma de esta materia se debería considerar expresamente estos instrumentos generales con carácter supletorio y como el parámetro mínimo a respetar en el tratamiento de datos personales por parte de la policía y los tribunales. Por último, no debemos olvidar que el Convenio 108 del Consejo de Europa sigue plenamente vigente y ha sido ratificado por todos los países miembros de la Unión. Dicho acuerdo supranacional se aplica tanto al ámbito público como al privado sin distinción, por tanto, debe ser considerado también al momento de determinar los estándares mínimos a respetar en la materia.[564]

Otro punto vinculado al ámbito de aplicación de la propuesta de Directiva, dice relación con el formato en que se soporta la información personal. Al respecto, la propuesta prescribe que sus disposiciones se aplican «al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero».[565] En consecuencia, sus disposiciones rigen para todo tipo de tratamiento, automatizado o manual. La inclusión de los tratamientos manuales, ya estaba recogida en la DM 2008/977/JAI y constituye un avance respecto de lo dispuesto en el Convenio 108 y la Recomendación

[563] Respecto de la Decisión Marco , en el mismo sentido véase, Cristina DIETRICH PLAZA, «Las tensiones entre libertad y seguridad en el marco jurídico actual de protección de datos de carácter personal en la Unión Europea», *ob. cit.*, p.195.

[564] Sobre este punto cabe recordar, que los propios marcos normativos de la Europol, Eurojust, SIS y VIS, entre otros, hacer referencia expresa al Convenio 108 de 1981 y a la Recomendación (87) 15 del Consejo de Europa, como parámetro mínimo a respetar en la materia.

[565] Artículo 2.2. de la propuesta de Directiva. En este punto, el proyecto sigue a la Decisión Marco 2008/977/JAI, que en su artículo 1.3. señala que sus disposiciones «se aplicará tanto al tratamiento automatizado como no automatizado, total o parcial, de datos personales que formen parte o esté previsto que vayan a formar parte de un fichero».

87(15) del Consejo de Europa[566], que sólo se aplican al tratamiento automatizado de datos, y lo acerca más al criterio de la Directiva 95/46/CE, que también contempla ambos tipos de tratamiento.

3. TRATADO DE PRÜM Y SU INCORPORACIÓN A LA NORMATIVA EUROPEA POR MEDIO DE LA DECISIÓN 2008/615/JAI

3.1 Origen y evolución de la normativa

La Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008 (en adelante, D2008/615/JAI)[567] tiene por objeto incorporar los aspectos esenciales de las disposiciones del Tratado de Prüm en el ordenamiento jurídico de la Unión Europea.[568] El Tratado de Prüm había sido suscrito entre algunos países europeos con la finalidad de profundizar la cooperación transfronteriza en materias de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal.[569] Es habitual que el Tratado de Prüm

[566] Cabe tener presente que la Recomendación 87(15) del Consejo de Europa, permite a los Estado miembro "ampliar" los principios contenidos en ella a los datos no tratados de forma automatizada.

[567] Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza. Publicada en el DOUE L 210/1 con fecha 6.8.2008. La ejecución técnica y administrativa de la Decisión 2008/615/JAI, se encuentra regulada en la Decisión 2008/616/JAI, también de 23 de junio de 2008. En ésta y su anexo, se establece el procedimiento para intercambio electrónico de datos de ADN, datos dactiloscópicos y datos de matriculación de vehículos, entre otros temas. Gran parte de su contenido coincide con el Acuerdo de ejecución del Tratado de Prüm. Este se aplica supletoriamente entre las partes que lo han suscrito respecto de las materias no reguladas por la Decisión 2008/616/JAI.

[568] Cfr. el considerando 1 de la Decisión 2008/615/JAI.

[569] Fue suscrito originalmente por entre Alemania, Bélgica, España, Francia, Luxemburgo, Holanda y Austria, el 27 de mayo de 2005. España lo ratificó el 18 de julio de 2006 y fue publicado en el BOE núm. 307, de 25 de diciembre de 2006. A los siete Estados originales firmantes del Tratado de Prüm, se le sumaron otros ocho: Italia, Portugal, Finlandia y Eslovenia Finlandia, Italia, Portugal, Eslovenia, Suecia, Romanía, Bulgaria y Grecia, que expresaron oficialmente su intención de acceder al mismo. Para un estudio detallado sobre el Tratado de Prüm, véase el número monográfico AAVV, «El Tratado de Prüm» en *Revista de Derecho Constitucional Europeo* (ReDCE), Número 7, Enero-Junio de 2007, y en particular, Emilio ACED FÉLEZ, "Ejercicio y garantía del derecho a la protección de datos personales en el Convenio de Prüm", *Revista de derecho constitucional europeo*, nº 7 (2007): pp. 65–96; Antonio BAR CENDÓN, "El Tratado de Prüm y la inmigración ilegal", *Revista de derecho constitucional europeo* N° 7 (2007): pp. 235–76; Gregorio Cámara CÁMARA VILLAR, "La garantía de los derechos fundamentales afectados por la Convención de Prüm", *Revista de derecho constitucional europeo*, nº 7 (2007): pp. 97–118; Cristina DIETRICH PLAZA, "El Tratado de Prüm en el marco de la regulación de la protección de datos personales en la Unión Europea", *Revista de derecho constitucional europeo*, nº 7 (2007): pp. 31–64; Teresa FREIXES SANJUÁN, "Protección de datos y globalización: la convención de Prüm", *Revista de derecho constitucional europeo* N° 7 (2007): pp. 11–20; Yolanda GÓMEZ SANCHEZ, "Los datos genéticos en el Tratado de Prüm", *Revista de derecho constitucional eropeo* N° 7 (2007): pp. 137–66; Manuel HEREDERO HIGUERAS, "La protección de los datos de interés policial y judicial en la Unión Europea: de Shengen a Prüm", *Revista Jurídica de Navarra*, 2006; Joan Lluís Pérez PÉREZ FRANCESCH, "Cooperación policial y judicial en la Convención de Prüm", *Revista de derecho*

sea llamado también «Schengen III», en el sentido de constituir la tercera fase de desarrollo del Acuerdo de Schengen de 1985[570] y el Convenio de aplicación de Schengen 1990, conocidos como «Schengen I» y «Schengen II», que pretendían desarrollar la cooperación entre los Estados Miembros de la UE.[571] Sin embargo, existe una diferencia esencial entre el Tratado de Prüm y los Acuerdos de Schengen. Al momento de suscribirse el acuerdo de Prüm ya existía un marco jurídico europeo que permitía a la Unión Europea regular estos asuntos, y más aún, al momento de su suscripción existían planes concretos de la Unión para regular los temas esenciales que abarca el Tratado de Prüm.[572] Por tanto, el hecho que hayan sido siete los Estados Miembros de la Unión Europea que firmaron el Tratado de Prüm, no es casual. Ello tendría por objeto saltarse el lento y fatigoso procedimiento de adopción de una «cooperación reforzada», en la forma como estaba establecida en el Tratado de la Unión Europea previo a la reforma del Tratado de Lisboa.[573] Esta intencionalidad se evidencia con el hecho que los responsables de Interior de once Estados Miembros de la UE mantuvieron una reunión previa a la celebración del Consejo de Ministros de Justicia y Asuntos de Interior del día 5 de diciembre de 2006. En dicha reunión se firmaron dos documentos: 1) El Acuerdo Técnico de Ejecución del Tratado de Prüm (ATIA), con el objetivo e incrementar la rapidez del intercambio de información entre las autoridades policiales de los Estados firmantes de Prüm; y 2) La Declaración Conjunta de los Ministros, firmada por los siete Estados firmantes del Tratado más cuatro que manifestaron su interés en adherirse al mismo: Italia, Portugal, Finlandia y Eslovenia, en la que se anuncia que durante la presidencia Alemana del primer semestre de 2007 se presentará una iniciativa para integrar las principales partes del Tratado en el acervo comunitario.

---

constitucional europeo, nº 7 (2007): pp. 119–36; José Carlos REMOTTI CARBONELL, "Las medidas contra el terrorismo en el marco del Tratado de Prüm", *Revista de derecho constitucional europeo* N° 7 (2007): pp. 181–206; Jacques ZILLER, "El tratado de Prüm", *Revista de derecho constitucional europeo*, nº 7 (2007): 21–30.

[570] El Acuerdo de Schengen fue firmado el 14 de junio de 1985, por Alemania, Francia, Bélgica, Holanda y Luxemburgo, con el objeto de acordar la supresión de las fronteras comunes.

[571] En la época del Schengen, dicha cooperación se desarrollaba dentro de la Comunidad Económica Europea (CEE).

[572] Cfr. Propuesta de Decisión Marco del Consejo sobre el intercambio de información en el marco del principio de disponibilidad, presentada por la Comisión con fecha 12 de octubre de 2005 - COM (2005) 490 final- la que finalmente no prosperó.

[573] Dada estas características de la forma en que se gestó el Convenio, Teresa FREIXES SANJUÁN, califica la Convención de Prüm como una «pseudo-cooperación reforzada», por no haber seguido las previsiones del Tratado de Niza para las cooperaciones reforzadas. Cfr. «Protección de datos y globalización: la convención de Prüm», op. cit., p. 12. En el mismo sentido, véase ZILLER, «El tratado de Prüm»; y PÉREZ FRANCESCH, «Cooperación policial y judicial en la Convención de Prüm».

Con el Convenio de Prüm se pone en práctica el «principio de disponibilidad», que tiene su origen en el Programa de la Haya.[574] En virtud de él, los agentes de los servicios de seguridad de un Estado de la Unión que necesite información para llevar a cabo sus funciones, debe poder obtenerla de otro Estado Miembro, y las autoridades de los servicios de seguridad de dichos Estados que tenga la información deben ponerla a su disposición para el fin declarado, teniendo en cuenta las necesidades de las investigaciones pendientes en dicho Estado Miembro.[575] En otros términos, se busca simplificar el acceso a información en poder de las autoridades de otro Estado Miembro con fines de prevención y represión penal.

Es evidente la relación entre el contenido del Tratado de Prüm y la Decisión que lo incorpora al acervo comunitario con el reforzamiento de las medidas de seguridad, motivadas por los atentados terroristas de 11 de septiembre de 2001 en Nueva York, 11 de marzo de 2004 en Madrid y 7 de julio de 2005 en Londres. En esta lucha es necesario remarcar que tanto la Unión como los Estados Miembros tienen como sustrato los principios del Estado democrático de derecho, lo que implica la necesidad de dar un tratamiento compatible entre la lucha eficaz contra el crimen y el respeto por los derechos y libertades fundamentales de sus ciudadanos. Llevando lo anterior al plano de la protección de datos personales, implica conciliar las medidas de lucha contra el terrorismo y la delincuencia organizada, con el debido respeto a la autodeterminación informativa de las personas, así como al resto de los derechos fundamentales recogidos en la CDFUE, el CEDH y las tradiciones constitucionales comunes de los Estados Miembros participantes. En otros términos, la búsqueda de una mayor cooperación entre

[574] El Programa de la Haya, busca la consolidación del espacio de libertad, seguridad y justicia en la Unión Europea. Fue adoptado por el Consejo Europeo celebrado el 4 y 5 de noviembre de 2004 y publicado en el DOUE nº C 53, de fecha 3 de marzo de 2005. Al respecto véase el apartado 1.3 del capítulo quinto de este trabajo, y Emilio ACED FÉLEZ, «La protección de datos en la cooperación policial europea : de la Recomendación (87) 15 al principio de disponibilidad: Título IV. Disposiciones Sectoriales. Cap. I. Ficheros de Titularidad Pública. artículos 22, 23.1 y 24.1», en *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, ed. Antonio TRONCOSO REIGADA (Navarra: Thomson-Civitas, 2010), pp. 1350-1388; Emilio ACED FÉLEZ, «Principio de disponibilidad y protección de datos en el ámbito policial», *Noticias Jurídicas*, abril de 2010, http://noticias.juridicas.com/articulos/15-Derecho%20Administrativo/201004-123095321697634.html;
José Francisco ETXEBERRÍA GURIDI, «Principio de disponibilidad y protección de datos personales: a la búsqueda del necesario equilibrio en el espacio judicial penal europeo», *Eguzkilore: Cuaderno del Instituto Vasco de Criminología* N° 23 (2009), pp. 351-366.

[575] El principio de disponibilidad ha sido recogido expresamente en el Considerando 4 de la Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, que incorpora parte del contenido de Prüm al ordenamiento jurídico de la Unión Europea.

los Estados Miembros para combatir la delincuencia, no los exime de su obligación de respetar los derechos humanos y libertades fundamentales propias de los Estados democráticos de derecho.[576]

3.2. Objeto y ámbito de aplicación

Tanto del Tratado de Prüm como la Decisión 2008/615/JAI, tienen por fin poner en práctica el principio disponibilidad.[577] Por ello, el objeto de ambos instrumentos es reforzar la cooperación transfronteriza europea entre las autoridades responsables de la prevención y la persecución de delitos, en particular en el campo del «intercambio de información» con la finalidad de combatir el terrorismo y la delincuencia transfronteriza.[578] En cuanto al ámbito de aplicación material de ambos instrumentos, podemos señalar que sus disposiciones se aplican: a) a las transferencia automatizada de perfiles de ADN, datos dactiloscópicos y ciertos datos de los registros nacionales de matriculación de vehículos; b) disposiciones sobre las condiciones de suministro de datos relacionados con acontecimientos importantes que tengan una dimensión transfronteriza; c) disposiciones relativas a las condiciones de suministro de información con el fin de prevenir atentados terroristas; d) disposiciones sobre las condiciones y procedimientos de intensificación de la cooperación policial transfronteriza a través de diversas medidas.[579] Respecto de su ámbito de aplicación territorial, el Tratado de Prüm disponía que se aplique al territorio de las partes contratantes situados en territorio europeo.[580] No obstante, se previó que si la Unión Europea adoptara normas que puedan afectar al ámbito de aplicación del Tratado, las disposiciones correspondientes de éste dejarán de aplicarse en beneficio del derecho de la Unión Europea[581], que fue precisamente lo que ocurrió al entrar en vigor la Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008.

---

[576] Al respecto véase Teresa FREIXES SANJUÁN, «Derechos fundamentales en la Unión Europea. Evolución y prospectiva: la construcción de un espacio jurídico europeo de los derechos fundamentales», *Revista de derecho constitucional europeo* N° 4 (2005), pp. 43-86.
[577] Cfr. Los considerando de ambos instrumentos.
[578] Cfr. El artículo 1 del Tratado de Prüm y de la Decisión 2008/615/JAI, así como los considerandos 1 y 21 de ésta última.
[579] Cfr. los Artículos 1.3. y 33.2 del Tratado de Prüm y artículo 1 y 24 de la Decisión 2008/615/JAI.
[580] Cfr. Artículo 45 del Tratado de Prüm.
[581] Cfr. Artículo 47.1. del Tratado de Prüm.

3.3. Nivel de protección otorgado a los datos personales

El Tratado de Prüm y la Decisión 2008/615/JAI, contienen un conjunto de disposiciones relativas al tratamiento de datos personales. En este apartado sólo analizaremos los aspectos generales relacionados con el nivel de protección de datos personales, reservando su análisis pormenorizado sobre el tratamiento de los mismos para los capítulos respectivos en la tercera parte de este trabajo.

En cuanto al nivel de protección de datos, ambos instrumentos realizan una remisión o reenvío a las normas del Consejo de Europa.[582] Se exige que cada Estado miembro garantice en su derecho interno un nivel de protección de datos equivalente, como mínimo, al que resulta del Convenio n° 108, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, el Protocolo adicional al Convenio de 8 de noviembre de 2001, y los principios de la Recomendación n° R(87) 15 del Consejo de Europa dirigida a regular la utilización de datos de carácter personal en el sector de la policía.

El recurso al bloque normativo del Consejo de Europa fue necesario porque al momento de suscribir el Tratado de Prüm y aprobarse la Decisión Marco 2008/615/JAI se carecía de una decisión marco sobre protección de datos en el denominado antiguo tercer pilar comunitario (cooperación policial y judicial). No obstante, la Decisión 2008/615/JAI supedita sus normas sobre protección de datos a una futura decisión marco que rija todos los ámbitos de la cooperación policial y judicial en materia penal, bajo la condición de que su nivel de protección de datos no sea inferior a la protección establecida por las normas del Consejo de Europa.[583] Ahora bien, la Decisión Marco 2008/977/JAI, dictada con la finalidad de regir el tratamiento de datos personales en el ámbito de la cooperación policial y judicial, excluyó de su ámbito de aplicación a la Decisión 2008/615/JAI.[584] Esta situación se mantiene en la propuesta de Directiva que pretende derogar y reemplazar a la DM 2008/977/JAI.[585] En consecuencia, el recurso a

[582] Cfr. Considerandos 19, 20 y artículo 25 de la Decisión 2008/615/JAI; y artículo 34 del Tratado de Prüm.
[583] Cfr. Considerando 20 de la Decisión 2008/615/JAI.
[584] Cfr. Considerando 39 de la Decisión Marco 2008/977/JAI.
[585] Al respecto, el artículo 59 de la Propuesta de Directiva COM (2012) 10 final, señala: «Las disposiciones específicas relativas a la protección de datos personales en lo que respecta al tratamiento de datos personales por parte de autoridades competentes a efectos de prevención, investigación, detección o

las disposiciones del Consejo de Europa para determinar el nivel mínimo a garantizar en el tratamiento de datos personales por parte de los órganos encargados de la prevención y represión penal, en los ámbitos de la lucha contra el terrorismo y la delincuencia transfronteriza regulados por la Decisión 2008/615/JAI, sigue plenamente vigente en la actualidad.

Otro punto que dificulta entregar un nivel de protección adecuado en el tratamiento de datos personales en la Decisión 2008/615/JAI es la forma como se accede a los datos y el control que se realiza de tales accesos. El acceso (transfronterizo) a las bases de datos de terceros países se realiza «en línea», en consecuencia, el Estado Miembro que gestiona un fichero no puede realizar comprobaciones previas, por lo que las verificaciones sobre el correcto uso del sistema sólo se pueden dar *a posteriori*.[586]

4. INSTITUCIONES COMUNITARIAS DE COOPERACIÓN POLICIAL Y JUDICIAL CON DISPOSICIONES PARTICULARES SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El marco regulatorio europeo de la protección de datos personales en el ámbito de la cooperación policial y judicial, se encuentra sumamente atomizado. Ante la ausencia de una norma de carácter «general» y «supletoria» que estableciera las bases generales para el tratamiento de los datos personales en el antiguo tercer pilar comunitario, han proliferado normas particulares para cada uno de los ámbitos que requieren tratar datos personales con fines de represión y prevención penal.

Si miramos 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, ésta se aplica a todas las actividades de tratamiento de datos personales en los Estados Miembros, tanto en el sector público como en el privado. Sin embargo, dicha Directiva excluye expresamente de su esfera de aplicación el tratamiento de datos personales efectuado

---

enjuiciamiento de infracciones penales o de ejecución de sanciones penales en actos de la Unión adoptados antes de la fecha de adopción de la presente Directiva que regulen el tratamiento de datos personales entre los Estados Miembros y el acceso de autoridades designadas de los Estados Miembros a los sistemas de información establecidos con arreglo a lo dispuesto en los Tratados en el ámbito de la presente Directiva no se verán afectadas».

[586] *Cfr*. Considerando 17 de la Decisión Marco 2008/615/JAI.

«en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario», como son las actividades en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial.

Por su parte, 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, que era teóricamente era la norma destinada a cumplir un rol similar a Directiva de 1995 en los ámbitos de la cooperación judicial y policial en materia penal, no cumplió su cometido atendido su limitado ámbito de aplicación. En efecto, dicha Decisión Marco de 2008 sólo comprende al tratamiento de los datos personales transmitidos o puestos a disposición entre los Estados Miembros. Es más, en ella expresamente se excluye varios actos adoptados en virtud del título VI del Tratado de la Unión Europea, entre ellos, las normas que rigen el funcionamiento de Europol, Eurojust, el Sistema de Información de Schengen (SIS), el Sistema de Información Aduanero (SIA), y los que permiten a las autoridades de los Estados Miembros acceder directamente a determinados sistemas de datos de otros Estados Miembros.[587]

Con la entrada en vigor del Tratado de Lisboa y la desaparición de la estructura de pilares comunitarios, tampoco se ha modificado sustancialmente, hasta ahora, el panorama previamente existente. De hecho, la propuesta de Directiva de 2012, que pretende derogar y reemplazar a la Decisión Marco 2008/977/JAI, perpetúa esta situación, manteniendo todas las excepciones a su ámbito de aplicación señalas precedentemente.[588] Creemos que ello evidencia una contradicción del Parlamento Europeo y el Consejo, ya que, por una parte, se predica en las iniciativas de reforma que ellas buscan homogenizar los niveles de protección de los datos personales en todos los ámbitos del derecho de la Unión, pero por otra, se establecen tantas excepciones que la aplicabilidad del marco general queda sumamente reducido.[589]

[587] Cfr. Considerando 39 de la Decisión Marco 2008/977/JAI.
[588] La gran novedad de la propuesta de Directiva en esta materia sería la incorporación de los tratamientos que realizan las policías de los Estados Miembros, es decir, la inclusión a su ámbito de aplicación de los tratamientos nacionales o domésticos.
[589] En el mismo sentido véase David ORDOÑEZ SOLÍS, *Privacidad y protección judicial de los datos personales* (Barcelona: Bosch, 2011), p. 79.

En consecuencia, si queremos tener una visión completa del tratamiento de datos personales en el ámbito en ámbito de la cooperación judicial y policial europea, debemos realizar una revisión, aunque sea somera, de la normativa específica que regula el tratamiento de datos personales en Europol y Eurojust, así como de las agencias europeas encargadas de la coordinación de la prevención y represión penal paneuropea[590], incluyendo de los grandes sistemas de almacenamiento y gestión de información, Eurodac; Sistema de Información Schengen (SIS); el Sistema de Información de Visados (SIV); el Sistema de Comparación de Huellas Dactilares (Eurodac); y el Sistema de Información Aduanera (SIA).[591]

El análisis de estas instituciones y sistemas de información se realizará principalmente desde la óptica de las modificaciones introducidas en las mismas por el Tratado de Lisboa, y de los cambios o adecuaciones normativas que ello comporta. Nos interesa sobre todo, determinar cuál es nivel de protección que se ofrece en ellos y verificar si esta atomización normativa del antiguo tercer pilar comunitario, en lo que respecta al tratamiento de datos personales, se debe a una efectiva especificidad de sus disposiciones que justifique su exclusión del régimen general de protección de datos; o por el contrario, obedece a la intención no declarada de crear ámbitos con regulación más laxa, que tolere mayores restricciones a los derechos de los ciudadanos y menores limitaciones y controles judiciales y administrativos, bajo el supuesto genérico e indeterminado de protección de la seguridad.[592]

[590] Tras la Comunicación de la Comisión «Agencias europeas – Orientaciones para el futuro», el Parlamento Europeo, el Consejo y la Comisión acordaron abrir un diálogo interinstitucional a fin de mejorar la coherencia, la eficacia y el trabajo de las agencias descentralizadas, lo que resultó en la creación de un Grupo de trabajo interinstitucional (GTI) en marzo de 2009, encargado de abordar una serie de cuestiones clave, entre otras, la función y la posición de las agencias en el panorama institucional de la UE, su creación, estructura y funcionamiento, la financiación, los presupuestos, la supervisión y la gestión. Esta labor llevó a adoptar un enfoque común aplicado a las agencias descentralizadas de la UE, aprobado por el Parlamento Europeo, el Consejo y la Comisión en julio de 2012, que deberá tenerse en cuenta en el contexto de todas las futuras decisiones relativas a las agencias descentralizadas de la UE, conforme a un análisis caso por caso. Cfr. COM (2008) 135; COM (2013) 535 final y COM (2013) 173 final.

[591] En este apartado sólo haremos referencia a los aspectos generales de la regulación del tratamiento de datos, reservando el análisis pormenorizado y comparativo en otras partes de este trabajo.

[592] Al respecto, véase Fernando IRURZUN MONTORO, «El diseño institucional de los órganos de cooperación en materia policial y judicial penal: COSI, Europol, Eurojust y el Fiscal Europeo», en *El derecho penal de la Unión Europea: situación actual y perspectivas de futuro*, de Luis Alberto Arroyo Zapatero, Adán Nieto Martín, y Marta Muñoz de Morales Romero (Cuenca: Ediciones de la Universidad de Castilla-La Mancha, 2007); y Patricia ESQUINAS VALVERDE, *Protección de datos personales en la Policía Europea* (Valencia: Tirant lo Blanch, 2010): pp. 23-31

4.1. La Oficina Europea de Policía (Europol)

La Oficina Europea de Policía (Europol) se creó inicialmente como un organismo intergubernamental en virtud de un Convenio celebrado en 1995[593] y que entró en vigor en 1999, con la finalidad de apoyar y reforzar la cooperación mutua entre Estados Miembros para prevenir y combatir el terrorismo y la delincuencia organizada.[594] El Convenio Europol ha sido modificado por varios textos posteriores que han ido entregando competencia a este organismo en diversas áreas.[595] Al igual que ha ocurrido con otros acuerdos iniciados por el mecanismo de las cooperaciones reforzadas, el Convenio Europol y sus modificaciones posteriores han sido incorporados a la normativa comunitaria por medio la Decisión 2009/371/JAI del Consejo, de 6 de abril de 2009 (en adelante, la Decisión Europol).[596] De esta forma Europol ha pasado a

[593] Cfr. Acto del Consejo de 26.7.1995 y Convenio basado en el artículo K.3 del Tratado de la UE, por el que se crea una Oficina Europea de Policía (Convenio Europol), ambos publicados en el DOCE n° C 316 de 27.11.1995. La idea de una Oficina Europea de Policía se mencionó por primera vez en el Consejo Europeo de Luxemburgo (junio de 1991), pero su creación se acordó en el Tratado de la Unión Europea, de 7 de febrero de 1992, basado en el artículo K.3. Sus labores comenzaron en enero de 1994 bajo la denominación de «Unidad de Drogas de Europol» (UDE). Posteriormente, en julio de 1995, se firmó el Convenio por el que se crea Europol, que entró en vigor el 1 de octubre de 1998.

[594] Europol nace como respuestas a dos fenómenos que se estaban desarrollando en Europa, la ampliación de la libre circulación de personas, unida al desarrollo de los fenómenos de la delincuencia organizada a nivel internacional, originando la necesidad de establecer una mayor cooperación entre los Estados en la lucha para combatir este fenómeno delictivo. Para un estudio detallado sobre las actividades de Europol, véase entre, otros Viorica-Andreea MARICA, «Génesis de Europol», *Ciencia policial: revista del Instituto de Estudios de Policía* nº 99 (2010): 3; Luis LUENGO ALFONSO, «Cooperación policial y Europol», en *El espacio europeo de libertad, seguridad y justicia*, de Ministerio del Interior (Madrid: Ministerio del Interior. Secretaría General Técnica, 2000), p. 103-116; Ricard MARTÍNEZ MARTÍNEZ, «Los datos de carácter personal en el convenio Europol: las comunicaciones de datos a terceros países», en *XIV Encuentros sobre Informática y Derecho: 2000-2001*, de Miguel Ángel DAVARA RODRIGUEZ (Pamplona: Aranzadi, 2001), pp. 129-162; Francisco Javier ARROYO ROMERO, *La influencia de Europol en la comunitarización de la policía europea* (Madrid: Akal, 2005); Juan SANTOS VARA, «El desarrollo de la Oficina Europea de Policía (EUROPOL): el control democrático y judicial », en *Los Tratados de Roma en su cincuenta aniversario: perspectivas desde la Asociación Española de Profesores de Derecho Internacional y Relaciones Internacionales* (Madrid: Marcial Pons, 2008), pp. 569-594; Andreea MARICA, «El sistema de tratamiento de la información en EUROPOL», *Institut de Ciències Polítiques i Socials* WP núm. 309 (2012): pp. 1-33.

[595] Cfr. Decisión del Consejo de 3.12.1998 (terrorismo) y Decisión del Consejo de 3.12.1998 (trata de seres humanos), ambos publicados en el DO n° C 26 de 30.1.1999; Acto del Consejo de 30.11.2000 (protocolo sobre el blanqueo de dinero), publicado en el DO n° C 358 de 13.12.2000; Acto del Consejo de 28.11.2002 (protocolo relativo a los equipos de investigación comunes), publicado en el DO n° C 312 de 16.12.2002; Acto del Consejo de 27.11.2003 (protocolo), publicado en el DO n° C 2 de 6.1.2004. Otros instrumentos europeos que otorgan competencia a Europol son: la Decisión 2005/511/JAI del Consejo, de 12 de julio de 2005, relativa a la protección del euro contra la falsificación, que designa a Europol como organismo central para la lucha contra la falsificación del euro. Publicado en el DO n° L 185 de 16.7.2005; y Decisión del Consejo, de 6 de diciembre de 2001, por la que se amplían las competencias de Europol a las formas graves de delincuencia internacional enumeradas en el anexo del Convenio Europol. Publicado en el DO n° C 362 de 18.12.2001.

[596] Publicada en el DOUE n° L 121 de 15.5.2009. Sobre la Decisión Europol, véase: Alexandra De MOOR, «The Europol Council Decision: Transforming Europol into an Agency of the European Union», *Common market law review* Vol. 47, Nº 4 (2010): pp. 1089-1121.

constituirse en una Agencia Europea financiada con cargo al presupuesto de la Unión. Con ello se buscaba, por una parte, simplificar y mejorar el marco jurídico de Europol y, por otra, reforzar la función del Parlamento Europeo en el control sobre Europol.[597]

Con la entrada en vigor del Tratado de Lisboa el 1 de diciembre de 2009, las disposiciones sobre Europol han pasado a formar parte del Tratado de Funcionamiento de la Unión Europea (Título V – Espacio de libertad, seguridad y justicia).[598] En concreto, el artículo 88 del TFUE, establece que Europol se regirá por un reglamento adoptado con arreglo al procedimiento legislativo ordinario. También estipula que los colegisladores fijarán procedimientos de control de las actividades de Europol por el Parlamento Europeo, control en el que participarán los Parlamentos Nacionales.

Cumpliendo el mandato del Tratado de Lisboa, en marzo de 2013, se presentó la propuesta de Reglamento relativo a la Agencia de la Unión Europea para la cooperación y la formación en funciones coercitivas (Europol) y por el que se derogan las Decisiones 2009/371/JAI que crea Europol y 2005/681/JAI que crea la Escuela Europea de Policía (en adelante, CEPOL).[599] La propuesta pretende fusionar en una sola institución europea la cooperación policial operativa de Europol con la experiencia en formación y educación de la CEPOL.[600]

[597] Cfr. Considerados 3 a 5 de la Decisión 2009/371/JAI.

[598] José Javier LASO PÉREZ, "Las relaciones exteriores de Europol tras la adopción de la Decisión de 2009 por la que se crea Europol y la entrada en vigor del Tratado de reforma de Lisboa". En La dimensión exterior del espacio de libertad, seguridad y justicia de la Unión Europea, de José MARÍN Y PÉREZ DE NANCLARES. Madrid: Iustel, (2012): pp. 314-354.

[599] La CEPOL fue creada como agencia de la UE en 2005, por la Decisión 2005/681/JAI, con la misión de llevar a cabo actividades relacionadas con la formación de los agentes con funciones coercitivas de las fuerzas de policía nacionales mediante la organización de cursos con una dimensión policial europea. Cfr. COM (2013) 173 final, de 27.3.2013.

[600] La intención del Consejo Europeo de convertir a Europol en «el eje para el intercambio de información entre las autoridades policiales de los Estados Miembros, un prestador de servicios y una plataforma para los servicios policiales», quedó explicito en el «Programa de Estocolmo», dónde se insta y reclama la creación de planes de formación y programas de intercambio europeos para todos los profesionales con funciones coercitivas a nivel nacional y de la UE, en los que la CEPOL debería desempeñar un papel fundamental con el fin de garantizar una dimensión europea. En la misma línea la Comisión en su Comunicación «La Estrategia de Seguridad Interior de la UE en acción: cinco medidas para una Europa más segura» (2), identificó una serie de retos, principios y directrices clave para abordar las cuestiones de seguridad en la UE, y sugirió una serie de acciones con la participación de Europol y la CEPOL para hacer frente a las amenazas a la seguridad que plantean la delincuencia grave y el terrorismo. Cfr. Programa de Estocolmo — Una Europa abierta y segura que sirva y proteja al ciudadano, Publicada en el DOUE n° C 115 de 4.5.2010; y la Comunicación de la Comisión al Parlamento Europeo y al Consejo "La Estrategia de Seguridad de la UE en acción: cinco medidas para una Europa más segura", COM (2010) 673 final, de 22.11.2010.

La propuesta de Reglamento plantea que la fusión de Europol y CEPOL en una sola agencia, ubicada en la sede actual de Europol en La Haya, podría crear sinergias importantes y mejorar su eficiencia, atendidos los conocimientos técnicos en cooperación policial operativa de Europol, sumado a la experiencia en formación y educación de la CEPOL. Los contactos entre el personal operativo y el personal de formación que trabajaría en una sola agencia, ayudarían a identificar las necesidades de formación, mejorando así la pertinencia y la focalización de la formación de la UE, en beneficio de la cooperación policial de la UE en su conjunto. Se evitaría de esta forma la duplicación de funciones de apoyo en ambas agencias y los ahorros resultantes podrían reasignarse e invertirse en funciones operativas y de formación básicas. Este aspecto reviste particular importancia en un contexto económico marcado por la escasez de los recursos nacionales y de la UE, y por la posibilidad de que no se disponga de otros medios para reforzar la formación en funciones coercitivas en la UE.[601]

El objetivo de Europol es apoyar y reforzar la acción de las autoridades competentes de los Estados Miembros y su cooperación mutua en materia de prevención y lucha contra la delincuencia organizada, el terrorismo y otras formas de delitos graves que afecten a dos o más Estados Miembros. Dicho organismo facilita el intercambio de información entre las autoridades con funciones coercitivas de los Estados Miembros, y proporciona análisis criminales para ayudar a las fuerzas de policía nacionales a llevar a cabo investigaciones transfronterizas.[602]

Su competencia abarca, entonces, sólo aquellos casos en que dos o más Estados Miembros requieran un planteamiento común para combatir los actos delictivos graves a los cuales hace referencia.[603] De esta forma, su rol pasa a ser el de ente responsable de coordinar la cooperación para la aplicación de la ley a escala de la Unión.[604] Para ello,

[601] Cfr. COM (2013) 173 final, de 27.3.2013, p. 4.
[602] Ídem.
[603] La Directiva ha ampliado las competencias y funciones de Europol. Ahora se incluyen un tipo de delincuencia que no está estrictamente relacionada con la delincuencia organizada, haciendo propia la misma lista de delitos graves que figura en la Decisión Marco del Consejo sobre la orden de detención europea, publicada en el DO L 190 de 18.7.2002, p. 1. También se ha ampliado su competencia a bases de datos remitida por entidades privadas. Cfr. los artículos 4, 5 y 25 y el anexo I de la Decisión Europol.
[604] Cfr. Artículo 3 y Considerando 23 de la Decisión 2009/371/JAI. Europol también desarrolla una intensa labor de cooperación internacional, lo que incluye el intercambio de datos personales, con terceros Estados, instituciones y organismos internacionales. Al respecto véase José Javier LASO PÉREZ, "Las relaciones exteriores de Europol tras la adopción de la Decisión de 2009 por la que se crea Europol y la entrada en vigor del Tratado de reforma de Lisboa". En La dimensión exterior del espacio de libertad,

cumple diversas funciones, entre las que destacan: notificar a los Estados miembros toda conexión entre delitos penales que les atañan; asistir a los Estados miembros en las investigaciones, proporcionar datos y prestar apoyo analítico; solicitar a los Estados miembros que inicien, emprendan y coordinen investigaciones sobre casos concretos y proponer equipos conjuntos de investigación; elaborar evaluaciones de las amenazas y otros informes; y recopilar, almacenar, tratar, analizar e intercambiar información.[605]

El tratamiento de datos personales es inherente a la actividad que desarrolla Europol. El actual sistema establecido por la Decisión de 2009, crea y regula la gestión de un «sistema de información general» y «ficheros de trabajo de análisis».[606] Los datos introducidos en estos sistemas pueden referirse tanto a personas involucradas en la comisión o que son sospechosas de planear algún delito, como también a información (datos) sobre testigos, víctimas, intermediarios, e incluso acompañantes del infractor. Los datos personales tratados deben estar directamente relacionados con tales personas (nombre, nacionalidad, número de la seguridad social, entre otros) y con los delitos cometidos.[607] Como se puede apreciar el espectro de personas cuyos datos pueden ser tratados por esta mega base de datos es bastante amplio. Es por ello que el establecimiento de un sistema claro de ejercicio de derechos a favor de los interesados (titulares de los datos), y la imposición de límites a las potestades de Europol, se transforman en un imperativo sino queremos caer en una sociedad del control preventivo perenne.[608]

---

seguridad y justicia de la Unión Europea, de José MARÍN Y PÉREZ DE NANCLARES. Madrid: Iustel, (2012): pp. 314-354..

[605] Cfr. Artículo 5 de la Decisión 2009/371/JAI.

[606] Cfr. Artículo 11 y y 14 de la Decisión. Al respecto el Considerando 14 de la misma Decisión, plantea que: «Las posibilidades actuales de Europol para crear y gestionar información de sistemas de tratamiento en apoyo de sus tareas deben ampliarse». Como resguardo propone que «tales sistemas adicionales de tratamiento de información de sistemas de tratamiento deben crearse y mantenerse de acuerdo con los principios generales de protección de datos contenidos en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, y en la Recomendación n o R (87) 15 del Comité de Ministros del Consejo de Europa, de 17 de septiembre de 1987, por medio de una decisión del consejo de administración de Europol».

[607] Sobre la gestión de estos ficheros véase Andreea MARICA, «El sistema de tratamiento de la información en EUROPOL», *Institut de Ciències Polítiques i Socials* WP núm. 309 (2012): pp. 6-30.

[608] En el mismo sentido Patricia ESQUINAS señala que «En una época de políticas internacionales ilógicas y desproporcionadas en materia de seguridad colectiva, que abarcan desde la libre disponibilidad para la Policía de las comunicaciones electrónicas privadas hasta el temido sistema de "escáner" en los aeropuertos, ni siquiera los más urgentes objetivos de lucha contra la delincuencia deberían servir, en una sociedad verdaderamente democrática, como coartada para lastimar la dignidad de la persona o sus garantías jurídicas esenciales. Así, considerando entre éstas el derecho individual a la autodeterminación informativa, concretamente el Sistema de Datos creado por la Policía Europea parece requerir de mayores controles jurisdiccionales y legales que aseguren al ciudadano ese derecho. En tal sentido, se propone una

Parte de estas aprensiones fueron tomadas en consideración al momento de elaborar la nueva propuesta de Reglamento que regirá Europol. En ella se rediseña la arquitectura de tratamiento de datos de la agencia, con el fin de mejorar los vínculos entre los datos en su posesión y su análisis posterior. Ya no se *predefinen* bases o sistemas de datos, sino que se adopta un enfoque de «protección de la privacidad desde el *diseño*» y de plena transparencia respecto al responsable de la protección de datos de Europol y el Supervisor Europeo de Protección de Datos. De esta forma se pretende conseguir altos estándares de seguridad y protección de los datos mediante garantías procedimentales aplicables a todo tipo específico de información. Además, el Reglamento establece detalladamente los fines del tratamiento de datos (controles cruzados, análisis estratégicos u otros de naturaleza general y análisis operativos en casos específicos), las fuentes de información y quiénes pueden tener acceso a los datos. También enumera las categorías de datos personales y de interesados, cuyos datos pueden ser recogidos para cada actividad de tratamiento de información específica. De esta forma, Europol podrá adaptar la arquitectura informática a los futuros retos y necesidades de los servicios con funciones coercitivas de la UE. Una vez en funcionamiento, esta nueva arquitectura permitirá a Europol vincular y analizar los datos pertinentes, reducir los retrasos en la identificación de tendencias y pautas y reducir la conservación múltiple de datos.[609]

En la Decisión Europol vigente, la operatividad de estos sistemas de información está a cargo de unidades nacionales, funcionarios de enlace y personal de Europol, los cuales pueden introducir y extraer datos directamente del sistema. Las unidades nacionales de Europol tienen «**acceso directo**» a todos los datos del sistema de información de Europol, a fin de evitar "trámites innecesarios" y asegurarse de que los datos que solicitan están disponibles.[610] Únicamente las autoridades competentes de los

---

reforma de su regulación vigente, a fin de garantizar el derecho de acceso a los datos personales, así como una efectiva tutela judicial frente a los actos de Europol». Cfr. Patricia ESQUINAS VALVERDE, *Protección de datos personales en la Policía Europea*.

[609] Cfr. COM (2013) 173 final, de 27.3.2013, p. 7.

[610] Cfr. Considerando 10 de la Decisión 2009/371/JAI. Con ello se reafirma el «principio de disponibilidad», consignado en el Programa de la Haya, como el principio rector en la actividades de Europol. Con arreglo a este principio, la información necesaria para luchar contra la delincuencia debe cruzar las fronteras interiores de la UE sin obstáculos. Al respecto véase el Supervisor Europeo de Protección de Datos, *Dictamen sobre la propuesta de Decisión del Consejo por la que se crea la Oficina Europea de Policía (Europol).* COM(2006) 817 final. Diario Oficial n° C 255 de 27.10.2007 p. 13-21, 27

Estados Miembros podrán tener acceso a todo dato de carácter personal procedente de Europol para prevenir y combatir la actividad delictiva.[611] Lo anterior cambia con el nuevo Reglamento de Europol, ya que la propuesta plantea que el acceso de los Estados Miembros a los datos personales en poder de Europol y los relativos a análisis operativos, se realizará en forma «**indirecta**» basado en un sistema de respuesta positiva o negativa, es decir, se realizará una comparación automatizada que generará una «respuesta positiva» anónima si los datos en poder del Estado Miembro solicitante concuerdan con los datos en poder de Europol. Si existe coincidencia, los correspondientes datos personales solo se facilitan en respuesta a una petición separada de seguimiento.

En lo que respecta al régimen jurídico aplicable al tratamiento de datos personales realizados por Europol, tanto la Decisión de 2009 como la propuesta de Reglamento de 2013, dedica un capítulo especial a su regulación, configurando, como se señaló, un corpus normativo especial.

Así, el capítulo V de la Decisión Europol de 2009 contiene normas sobre protección de datos y seguridad de los datos, que pueden considerarse *lex specialis*, generadoras de nuevas normas aplicables por encima de la *lex generalis*. Sin embargo, como es sabido, al momento de dictarse la Decisión Europol aún no había sido adoptado para el tercer pilar (en un sentido material o de fondo, aún no se dicta) el marco jurídico general. Se suponía que éste estaría dado por la Decisión Marco 2008/977/JAI del Consejo, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. Pero atendido su limitado ámbito de aplicación, que comprende sólo «la transferencia de datos personales por los Estados Miembros a Europol», es dudoso el calificativo de marco general. Además, ésta Decisión excluye expresamente de su ámbito de aplicación al conjunto de disposiciones pertinentes en materia de protección de datos de la Decisión Europol, bajo el argumento de que ésta última «contiene disposiciones específicas sobre protección de datos

---

de octubre de 2007, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006XX1027(02):ES:HTML; Anselmo Del MORAL TORRES, «La cooperación policial en la Unión Europea: propuesta de un modelo europeo de inteligencia criminal», *Análisis del Real Instituto Elcano (ARI)* n.º 50 (2010): 1-12.

[611] El artículo 3 de la Decisión Europol de 2009, define a las autoridades competentes «como todos los organismos públicos existentes en los Estados Miembros que sean responsables, conforme al Derecho nacional, de la prevención y lucha contra los delitos».

personales que regulan estas cuestiones de forma más pormenorizada, debido a la naturaleza, las funciones y las competencias particulares de Europol».[612]

La Propuesta de Reglamento Europol de 2013, por su parte, consolida el régimen jurídico autónomo o especial en lo que se refiere a la de protección de datos personales en las labores que desempeña. Dicho régimen particular de regulación del tratamiento de datos personales tiene como base jurídica la declaración 21 adjunta al Tratado de Lisboa, que reconoce la especificidad del tratamiento de los datos personales en el contexto de las funciones coercitivas.

No obstante, se introduce un cambio importante respecto de la Decisión de 2009, en el sentido que se establece como régimen supletorio los principios en los que se basa el Reglamento (CE) nº 45/2001, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, disposición que pasa a tener un rol más protagónico. En efecto, en la Decisión Europol de 2009 sólo hace una remisión al Reglamento 45/2001, en lo relativo al «nombramiento y funciones del responsable de la protección de datos en Europol»[613]. En cambio, la nueva propuesta de Reglamento Europol realiza un reenvío más amplio al Reglamento de 2001, al hacer aplicables al tratamiento de datos realizados por Europol «los principios en los que se basa el Reglamento 45/2001».[614]

Además, se declara que las normas de protección de datos en el nuevo Reglamento de Europol se han adaptado a los instrumentos de protección de datos aplicables en el ámbito de la cooperación policial y judicial. En concreto, se cita al Convenio nº 108, la Recomendación nº R (87) 24 del Consejo de Europa, y de la Decisión Marco 2008/977/JAI del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial, incluyendo la Directiva que derogará y reemplazará a ésta última. De esta forma se trata de garantizar un alto nivel de protección de las personas físicas en lo que respecta al tratamiento de los datos

[612] Cfr. Considerando 12 de la Decisión.
[613] Cfr. Considerando 13 de la Decisión Europol de 2009, p. 38.
[614] Cfr. COM (2013) 173 final, de 27.3.2013, p. 9

personales, al tiempo que se tiene debidamente en cuenta la especificidad de las funciones coercitivas.[615]

Por último, es importante consignar el cambio que trae la propuesta de Reglamento Europol en materia de control de sus actividades vinculadas al tratamiento de datos personales. La Decisión Europol de 2009 radicó esta función en una Autoridad común de control, denominada «Supervisor de Protección de Datos de Europol», institución que ha sido criticada en relación a sus reales, independientes y exiguos poderes de intervención. Es por ello, que la propuesta de Reglamento Europol de 2013, entrega esta labor de supervisión y control al Supervisor Europeo de Protección de Datos.[616] Se garantiza así el pleno cumplimiento de los criterios de independencia establecidos en la jurisprudencia del Tribunal de Justicia y, debido a las competencias ejecutivas del SEPD, la efectividad de la supervisión de la protección de datos.[617]

Sin perjuicio de lo anterior, las autoridades nacionales de protección de datos siguen siendo competentes para supervisar la introducción, extracción y comunicación a Europol de datos personales por un Estado Miembro. También siguen siendo responsables de examinar si dicha introducción, extracción o comunicación vulneran los derechos del interesado.[618] Además, la propuesta de Reglamento introduce elementos de «supervisión conjunta» sobre los datos transferidos *a* y tratados *por* Europol, en cuestiones específicas que requieran una participación nacional y a fin de garantizar una aplicación coherente del Reglamento en toda la Unión Europea. De esta forma, el Supervisor Europeo de Protección de Datos y las autoridades nacionales de control deben cooperar cada uno dentro de sus competencias para el logro de sus fines.[619]

---

[615] Cfr. COM (2013) 173 final, de 27.3.2013, p. 9 y 18. Cabe recordar que la Decisión Europol de 2009, también realiza un reenvío a las disposiciones del Consejo de Europa, en los siguientes términos: «Sin perjuicio de las disposiciones específicas de la presente Decisión, Europol tendrá en cuenta los principios del Convenio del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, y la Recomendación n o R (87) 15, de 17 de septiembre de 1987, del Comité de Ministros del Consejo de Europa». Cfr. Capítulo V (artículos 27-35) y considerandos 11 y 14 de la Decisión Europol.

[616] El artículo 46 de la propuesta de Reglamento Europol de 2013, plantea en numeral 1: «El Supervisor Europeo de Protección de Datos se encargará de vigilar y asegurar la aplicación de las disposiciones del presente Reglamento relativas a la protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos personales por Europol, y de asesorar a Europol y a los interesados sobre cualquier cuestión».

Artículo 49 Derecho a presentar una queja ante el Supervisor Europeo de Protección de Datos

[617] Cfr. COM (2013) 173 final, de 27.3.2013, p. 6-10.

[618] Ídem.

[619] Cfr. los Considerando 41, 42 y 44 de la COM (2013) 173 final, de 27.3.2013, p. 19.

4.2. La Unidad de Cooperación Judicial (Eurojust)

La Unidad de Cooperación Judicial Europea (en adelante, Eurojust) fue creada por la Decisión 2002/187/JAI[620] del Consejo, con la finalidad de reforzar la lucha contra las formas graves de delincuencia en la Unión Europea, mediante la coordinación entre las autoridades judiciales competentes de los Estados Miembros. La normativa de Eurojust ha sido modificada en dos oportunidades, mediante la Decisión 2003/659/JAI[621] y por la Decisión 2009/426/JAI.[622] Esta última, implicó una amplia reforma a las actuaciones y funcionamiento de Eurojust.[623]

El Tratado de Lisboa hace una referencia expresa a las funciones a desarrollar por Eurojust y la forma en que se debe regular su actividad. En el artículo 85.1 del Tratado de Funcionamiento de la UE (TFUE) se reconoce de manera explícita la misión de Eurojust para apoyar y reforzar la coordinación y cooperación entre las autoridades fiscalizadoras y de investigación nacionales en relación con delitos graves que afecten a dos o más Estados Miembros, o que deban perseguirse según criterios comunes. El mismo artículo también prevé que la estructura, el funcionamiento, el campo de acción y las labores de Eurojust se deben definir conforme a reglamentos adoptados con arreglo al procedimiento legislativo ordinario. De esta forma se valida el control democrático sobre Eurojust, ya que tanto el Parlamento Europeo como los parlamentos nacionales pueden intervenir en la evaluación de sus actividades.

En cumplimiento del mandato ordenado por el artículo 85 del TFUE, actualmente se encuentra en proceso de elaboración una propuesta de Reglamento que

[620] Publicada en el DOCE n° L 63/1 de 6.3.3002.
[621] Publicada en el DOUE n° L 245/44 de 29.9.2003.
[622] Decisión 2009/426/JAI del Consejo de 16 de diciembre de 2008, publicada en el DOUE n° L 138 de 4.6.2009, p. 14. El plazo de transposición se extendía hasta el 4 de junio de 2011.
[623] En este apartado sólo trataremos los aspectos esenciales del tratamiento de datos personales por parte de Eurojust, poniendo énfasis en las transformaciones que ha traído el Tratado de Lisboa en la materia. Para un estudio detallado sobre las actividades desarrolladas por este órgano comunitario, véase entre otros, Nicolás ALONSO MOREDA, «Eurojust, a la vanguardia de la cooperación judicial en materia penal en la Unión Europea», *Revista de Derecho Comunitario Europeo* Año n^{o} 16, N^{o} 41 (2012): pp. 119-157; David ORDOÑEZ SOLÍS, *Privacidad y protección judicial de los datos personales*; María Carmen TIRADO ROBLES, «El refuerzo de la cooperación judicial penal en la Unión Europea: comentario a la Decisión del Consejo 2009/426/JAI, de 16 de diciembre de 2008», *Revista General de Derecho Europeo* n^{o} 21 (2010), disponible en: http://dialnet.unirioja.es/servlet/articulo?codigo=3279047 [consultado el 12.01.2014].

contempla todos estos elementos y ofrece un marco jurídico exclusivo y renovado para una nueva agencia de cooperación en materia de Justicia Penal (Eurojust), que será el sucesor legal de la estructura Eurojust establecida por la Decisión 2002/187/JAI del Consejo.[624] Dicha propuesta, preserva algunos elementos que han demostrado ser eficientes en la gestión y el funcionamiento de Eurojust, actualiza su marco jurídico y optimiza su funcionamiento y estructura en consonancia con el Tratado de Lisboa y las disposiciones del enfoque común de las Agencias Europeas en el Espacio de Libertad, Seguridad y Justicia.[625]

Los principales objetivos de la propuesta de Reglamento Eurojust son: aumentar la eficiencia de Eurojust dotándolo de una nueva estructura de gobernanza; mejorar la eficacia operativa de Eurojust mediante una definición homogénea del estatus y las competencias de los miembros nacionales; prever la función del Parlamento Europeo y de los parlamentos nacionales en la evaluación de las actividades de Eurojust en consonancia con el Tratado de Lisboa; adaptar el marco jurídico de Eurojust al enfoque común, a la vez que se preserva íntegramente su papel especial en la coordinación de las investigaciones penales en curso; y garantizar que Eurojust pueda cooperar estrechamente con la Fiscalía Europea una vez que esta se haya creado.[626]

En lo que respecta al régimen aplicable al tratamiento de los datos personales, la propuesta de Reglamento realiza una triple distinción entre tratamiento realizados por Eurojust en el marco de sus actividades, los datos transferidos desde los Estados Miembros a Eurojust y, por último, respecto de las transferencias internacionales de datos desde Eurojust a organismos internacionales o terceros Estados.

---

[624] Cfr. la Propuesta de Reglamento del Parlamento y del Consejo «sobre la Agencia Europea de Cooperación en materia de Justicia Penal (Eurojust)», COM (2013) 535 final, de fecha 17.7.2013.

[625] Al respecto véase la Comunicación de la Comisión «Agencias europeas – Orientaciones para el futuro», COM (2008) 135. En esta línea de enfoque común, la propuesta de Reglamento de Eurojust contempla remisiones tanto a la propuesta de Reglamento por la que se crea la Fiscalía Europea como la que modifica Europol. Sobre la nueva propuesta de Reglamento de Europol, se ha generado diversos debates, véase el seminario estratégico «Eurojust and the Lisbon Treaty. Towards more effective action», celebrado en Brujas, del 20 al 22 de septiembre de 2010; la conferencia Eurojust-ERA «10 Years of Eurojust: Operational Achievements and Future Challenges», que se celebró en La Haya los días 12 y 13 de noviembre de 2012. Además, el futuro de Eurojust se debatió en una reunión informal especial del Consejo celebrada en febrero de 2012 con motivo del décimo aniversario de Eurojust. También se han recopilado opiniones de las partes interesadas en un estudio titulado «Study on the strengthening of Eurojust», encargado por la Comisión, que ofrece una buena perspectiva de los problemas existentes y presenta varias alternativas políticas para solucionarlos.

[626] Cfr. COM (2013) 535 final, p. 4.

Sobre el primer punto, el Capítulo IV de la propuesta de Reglamento, denominado «tratamiento de la información», establece al Reglamento (CE) nº 45/2001[627] como el régimen aplicable para el tratamiento de todos los datos personales en Eurojust, es decir, se establece como norma supletoria general las disposiciones del Reglamento de 2001 respecto del tratamiento de datos personales realizados en el marco de las actividades de Eurojust. Sin perjuicio de ello, la propuesta de Reglamento Eurojust establece una serie de normas particulares y complementarias para el tratamiento datos personales «operativos» propios de las actividades de cooperación judicial.[628] Lo anterior constituye un cambio importante respecto de las normas anteriores que regulaban el tratamiento de datos personales por parte de Eurojust, ya que las Decisiones de 2002, 2003 y 2009, reenviaban a las disposiciones del Consejo de Europa como la norma mínima a respetar en cuanto al nivel de protección que se debía respetar en el Tratamiento de datos personales en las actividades de Eurojust. De esta forma, la norma general y supletoria en la materia pasa a ser una norma de la Unión (Reglamento 45/2001), dando mayor coherencia y uniformidad al sistema de protección de datos que se pretende construir el Postratado de Lisboa.

No obstante lo anterior, para determinar el estándar mínimo aplicable al tratamiento que las autoridades de los Estados Miembros hacen de los datos personales y la transferencia de dicha información a Eurojust, se seguirá recurriendo al Convenio nº 108 del Consejo de Europa. Ahora bien, el recurso al marco normativo del Consejo de Europa, como norma supletoria y general del tratamiento nacional o domestico de los datos personales por parte de la policía, debería cambiar con la entrada en vigor de la Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos, ya que esta Directiva se aplica

[627] Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. Publicado en el DOCE n° L 8 de 12.1.2001, p. 1.

[628] La propuesta de Reglamento propone que se autorice a Eurojust para tratar datos personales de aquellas personas que, de conformidad con la legislación nacional de los Estados Miembros de que se trate, sean sospechosos de haber cometido, participado o haber sido condenados por un delito penal, respecto del cual Eurojust sea competente. Cfr. Considerando 22 de la propuesta de Reglamento Eurojust, p. 11.

tanto al tratamiento nacional como a las transferencias que se realizan desde los Estados de la Unión a Europol como a Eurojust.[629]

Por último, cuando Eurojust transfiera datos personales a una autoridad de un tercer país o a una organización internacional o a Interpol en virtud de lo dispuesto en un acuerdo internacional concluido con arreglo al artículo 218 del Tratado, las garantías adecuadas aplicables con respecto a la protección de la privacidad y los derechos y las libertades fundamentales de las personas, deben velar por el cumplimiento de las disposiciones contenidas en el presente Reglamento relativas a la protección de datos.[630]

Otro cambio significativo de la propuesta, referido al tratamiento de datos personales, es el alineamiento de las disposiciones sobre los derechos de los interesados con el Reglamento (CE) nº 45/2001. Además, se toman en consideración las normas de protección previstas en el conjunto de medidas de reforma del ámbito de la protección de datos, adoptado por la Comisión en enero de 2012.[631] Asimismo, se prevé un cambio importante en el mecanismo de supervisión, al establecer al Supervisor Europeo de Protección de Datos (SEPD) como el organismo encargado de la supervisión del tratamiento de todos los datos personales en Eurojust. De esta forma, el SEPD asumiría las labores de la autoridad común de control establecidas en el marco de la Decisión del Consejo relativa a Eurojust.[632]

4.3. Agencia Europea para la gestión de la cooperación operativa en las fronteras exteriores de los Estados miembros de la Unión Europea (Frontex)

La Agencia Europea para la gestión de la cooperación operativa en las fronteras exteriores (en lo sucesivo, Frontex) fue creada por el Reglamento (CE) n° 2007/2004 del Consejo, de 26 de octubre de 2004, y comenzó sus operaciones en mayo de 2005 con el fin de mejorar la gestión integrada de las fronteras exteriores de los Estados

[629] Cfr. COM (2012) 10 final, de 25.1.2012 y Considerando 20 de la Propuesta de Reglamento Eurojust COM (2013) 535 final, p. 5, 6 y 10.
[630] Cfr. COM (2013) 535 final, p. 10.
[631] Cfr. Comunicación COM (2012) 9 final sobre «el enfoque del nuevo marco jurídico para la protección de los datos personales en la UE».
[632] Sobre la labor desarrollada por la Autoridad Común de Control (ACC) en Eurojust, véase http://eurojust.europa.eu/doclibrary/Eurojust-framework/jsb/jsb/The%20Role%20of%20the%20Joint%20Supervisory%20Body%20of%20Eurojust%20%28leaflet%29/Role-of-JSB-ES.pdf [consulta 8.9.2013]

Miembros de la Unión Europea.[633] Sus disposiciones han sido modificadas en varias oportunidades. La primera, mediante el Reglamento (CE) n° 863/2007 del Parlamento Europeo y del Consejo, de 11 de julio de 2007, por el que se estableció un mecanismo para la creación de equipos de intervención rápida en las fronteras[634] y, la última, en 2011, mediante el Reglamento 1168/2011, del Parlamento Europeo y del Consejo, de 25 de octubre de 2011.[635]

En términos generales, podemos señalar que la política comunitaria en materias de fronteras exteriores tiene por objeto establecer una gestión integrada, mediante normas y procedimientos comunes, que garantice un nivel elevado y uniforme de control y vigilancia, corolario indispensable de la libre circulación de personas en la Unión Europea y componente esencial del espacio de libertad, seguridad y justicia.[636]

Como hemos visto en los apartados anteriores, todos los órganos de la Unión que gestionan bases de datos de alcance transnacional, usan datos personales. Dado los límites de este trabajo, sólo nos abocaremos a la revisión de las disposiciones relativas al tratamiento de datos personales que realiza Frontex en el cumplimiento de sus funciones y, particularmente, pondremos el foco en el nivel de protección que se ofrece, en las garantías al derecho fundamental a la protección de datos personales, y en los mecanismos de control establecidos para ello.

---

[633] Publicado en el DOCE n° L 349 de 25.11.2004, p.1.
[634] Publicado en el DOCE n° L 199 de 31.7.2007, p. 30.
[635] Publicado en el DOUE n° L 304, de fecha 22.11.2011, p. 1.
[636] Para un estudio detallado del origen, evolución y actividades desarrolladas por Frontex, véase entre otros: Rubén ANDERSSON, «Frontex y la creación de la frontera euroafricana: golpeando la valla ilusoria», *Revista de derecho migratorio y extranjería* n° 28 (2011): pp. 177-191; Rut BERMEJO CASADO, «El proceso de institucionalización de la cooperación en la gestión operativa de las fronteras externas de la UE: La creación de Frontex», *Revista CIDOB d'afers internacionals* n° 91 (2010): pp. 29-62; Laura GARCÍA GUTIERREZ, «TJCE - Sentencia de 18.12.2007, Reino Unido / Consejo, C-77/2005. Creación de la Agencia Frontex - Validez - Exclusión del Reino Unido - Acervo y Protocolo de Schengen», *Revista de Derecho Comunitario Europeo* Año 13, n° 34 (2009): pp. 1083-1093; Jorge Antonio QUINDIMIL LÓPEZ, «La Unión Europea, FRONTEX y la seguridad en las fronteras marítimas. ¿Hacia un modelo europeo de "seguridad humanizada" en el mar? », *Revista de Derecho Comunitario Europeo* Año n° 16, n° 41 (2012): pp. 57-118; Claire RODIER, «Frontex, el brazo armado de la Europa fortificada», *El estado del mundo: anuario económico geopolítico mundial* n° 27 (2011): pp. 135-139; José Luis TORRES, «Uso de las nuevas tecnologías en la gestión integral de fronteras realizado pro FRONTEX para combatir la criminalidad organizada transnacional», en *La seguridad y la defensa en el actual marco socio-económico: nuevas estrategias frente a nuevas amenazas*, ed. Miguel Requena y Díez de Revenga (Madrid: Instituto Universitario General Gutiérrez Mellado, 2011), pp. 217-244; Mariola URREA CORRES, «El control de fronteras de la Unión Europea y su dimensión exterior: algunos interrogantes sobre la actuación de FRONTEX», en *La dimensión exterior del espacio de libertad, seguridad y justicia de la Unión Europea* (Madrid: Iustel, 2012), 235-254; Mariola URREA CORRES, «El control de fronteras exteriores como instrumento para la seguridad: una aproximación al nuevo marco jurídico de frontex », *Revista del Instituto Español de Estudios Estratégicos* n° 0 (2012): pp. 153-172.

La agencia Frontex, posee un sistema de información de datos personales para ejecutar sus funciones. Esta situación se ha visto reforzada por la modificación de 2011, donde expresamente se autoriza el tratamiento de datos personales de las personas que son devueltas a sus países de origen, en las llamadas «operaciones de retorno», así como aquellas otras sospechosas de estar implicadas en actividades delictivas transfronterizas, en actividades de inmigración ilegal o en actividades de trata de personas.[637] También se regula el intercambio de datos personales con la Comisión, los Estados Miembros, con otras agencias de la Unión y organismos internacionales.[638]

En primer lugar, debemos señalar que como toda norma reglamentaria europea, esta encuentra sus límites en el respeto de los derechos y libertades de las personas, reconocidos por el TFUE y la Carta de los Derechos Fundamentales; y dada la naturaleza de la labor desarrollada por Frontex se debe una especial observación y respeto del derecho a la dignidad humana, la prohibición de la tortura y de las penas o los tratos inhumanos o degradantes, el derecho a la libertad y a la seguridad, el derecho a la protección de los datos personales, el derecho de asilo, el principio de no devolución, el principio de no discriminación, los derechos del menor y el derecho a la tutela judicial efectiva.[639]

En lo que respecta al marco normativo aplicable al tratamiento de datos personales que se realizan para el control de las fronteras exteriores, debemos realizar una distinción. Si el tratamiento lo realiza Frontex en el cumplimiento de sus funciones[640], se aplican las disposiciones del Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las

[637] Cfr. artículos 11, 11 *bis*, 11 *ter*, 11 *cuater* del Reglamento Frontex de 2011.
[638] El artículo 13 del Reglamento Frontex de 2011, dispone en su apartado primero que: «La Agencia podrá cooperar con Europol, la Oficina Europea de Apoyo al Asilo, la Agencia de los Derechos Fundamentales de la Unión Europea ("Agencia de los Derechos Fundamentales"), otras agencias y órganos de la Unión y con las organizaciones internacionales competentes en los ámbitos regulados por el presente Reglamento, en el marco de acuerdos de trabajo celebrados con dichos organismos, de acuerdo con las disposiciones pertinentes del TFUE y con las disposiciones sobre la competencia de dichos organismos. La Agencia informará sistemáticamente al Parlamento Europeo sobre tales acuerdos».
[639] Cfr. Considerando 29 del Reglamento Frontex de 2011.
[640] Cfr. Capitulo II (artículos 2 a 14) del Reglamento Frontex de 2004.

instituciones y los organismos comunitarios y a la libre circulación de estos datos.[641] En cambio, cada Estado es responsable del tratamiento de los datos personales que se realicen en sus fronteras exteriores. Como esta materia está directamente vinculada a la libre circulación de las personas en el espacio Europeo, le son plenamente aplicables las disposiciones de 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, así como las normas generales y específicas que cada Estado haya dictado para regular la protección de datos en general, y en particular para la gestión y control de sus fronteras exteriores.[642]

En lo que se refiere a los organismo de control, la normativa Frontex, establece que el Supervisor Europeo de Protección de Datos debe vigilar el tratamiento de datos personales que efectúe la Agencia y tener competencia para obtener de la misma el acceso a toda la información necesaria para efectuar sus investigaciones.[643] También se le otorga al SEPD un rol de garante *ex ante* sobre los intercambios (transmisión y comunicación) de datos personales entre Frontex y otras agencias u organismos de la Unión. Con ello los acuerdos de trabajo específicos en materia de intercambio de datos personales quedan limitados a la aprobación previa del Supervisor Europeo de Protección de Datos.[644] Por último, en cumplimiento del Reglamento (CE) n° 45/2001, el Consejo de Administración de Frontex debe establecer un agente que vele por el respeto del derecho fundamental a la protección de los datos personales.[645]

5. SISTEMAS INFORMÁTICOS DE GRAN MAGNITUD EN EL ESPACIO DE JUSTICIA, LIBERTAD Y SEGURIDAD

El artículo 67 del TFUE dispone que la Unión deba garantizar la ausencia de controles de las personas en las fronteras interiores y desarrollará una política común de asilo, inmigración y control de las fronteras exteriores. Por su parte, el artículo 77 del TFUE exige la adopción de medidas relativas a la política común de visados, los

[641] Cfr. Considerando 19 del Reglamento Frontex de 2004, y considerando 25 del Reglamento Frontex de 2011.
[642] Cfr. Considerado 26 y el artículo 11 *quater* del Reglamento Frontex de 2011.
[643] Cfr. Considerando 25 del Reglamento Frontex de 2011.
[644] Cfr. Art. 13 Reglamento Frontex de 2011.
[645] Cfr. Artículo 11 *bis* y 26 *bis* del Reglamento Frontex de 2011.

controles a los cuales se someterá a las personas que crucen las fronteras exteriores, las condiciones en las que los nacionales de terceros países podrán circular libremente por la Unión, cualquier medida necesaria para el establecimiento progresivo de un sistema integrado de gestión de las fronteras interiores, y la ausencia total de controles de las personas, sea cual sea su nacionalidad, cuando crucen las fronteras interiores.[646]

En cumplimiento de dichos fines, en los últimos años se han desarrollado un número importante de sistemas informáticos de gran magnitud (SIS, VIS, Eurodac, entre otros) vinculados directa o indirectamente a la supresión de las fronteras interiores de la Unión Europea. Aunque cada uno tiene un propósito diferente, estos sistemas de información comparten ciertas características comunes, tales como el tamaño y la interacción entre unidades nacionales, unidades centrales y con otros organismos de la Unión, e incluso con terceros países y organismos internacionales.[647]

Con la finalidad de mejorar la gestión operativa de éstos sistemas de información, el Parlamento Europeo y el Consejo, mediante el Reglamento (UE) N° 1077/2011, de 25 de octubre de 2011, crearon una agencia europea para la gestión operativa a largo plazo de los sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia (en adelante, EUROSIGMA), que se encarga de la gestión operativa del Sistema de Información de Schengen de segunda generación (SIS II), del Sistema de Información de Visados (VIS) y de Eurodac.[648]

---

[646] Al respecto cabe recordar, que ya en el Programa de La Haya (2005-2009) se hacía un llamamiento para mejorar el acceso a los sistemas de ficheros de datos existentes en la Unión. En la misma línea, el Programa de Estocolmo (2010-2014) pidió que al recopilar los datos se tuviera bien claro cuáles eran los objetivos y que el desarrollo del intercambio de información y sus herramientas se guíe por las necesidades de aplicación de la ley. Cfr. Reglamento (UE) Nº 603/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, Publicado en el DOUE nº L 180 de 29.6.2013, p. 2.

[647] Los marcos jurídicos de SIS II, VIS y EURODAC se caracterizan por lo que se ha denominado «geometría variable», es decir, que se ven afectados por el conjunto de Protocolos adicionales al Tratado de Funcionamiento de la Unión Europea, donde se establecen las posiciones del Reino Unido, Irlanda y Dinamarca, sobre el desarrollo del acervo Schengen. Así por ejemplo, Irlanda y el Reino Unido forman parte de EURODAC, pero sólo participan parcialmente en el SIS II y no participan en el SIV, mientras que Dinamarca participa en los tres sistemas con arreglo a una base jurídica diferente. Por otra parte, países no pertenecientes a la UE como Islandia, Noruega, Suiza y Liechtenstein, participan o participarán en la ejecución, aplicación y desarrollo del acervo de Schengen y, por tanto, participan tanto en el SIS II como en el SIV. Cfr. COM (2010) 93 final, pp. 3-11.

[648] El Reglamento (UE) N° 1077/2011, fue publicado en el DOUE n° L 186, de 1.11.2011. La base jurídica del Reglamento fueron: el artículo 77, apartado 2, letras a) y b), el artículo 78, apartado 2, letra e), el artículo 79, apartado 2, letra c), el artículo 74, el artículo 82, apartado 1, letra d) y el artículo 87, apartado 2, letra a), del Tratado de Funcionamiento de la Unión Europea. Sobre el proceso de elaboración de este Reglamento, véase: la COM (2010) 93 final, «propuesta modificada de reglamento (ue) nº …/…del Parlamento Europeo y del Consejo por el que se crea una Agencia para la gestión operativa de

La tarea esencial de esta Agencia europea es de carácter «operativa», lo que significa garantizar la gestión global de los sistemas de información y su funcionamiento durante 24 horas al día, siete días a la semana, y de este modo, garantizar un flujo de intercambio de datos continuo y sin interrupciones.[649] Además de estas tareas operativas, se asignarán a la Agencia las competencias correspondientes en materia de adopción de medidas de seguridad, presentación de informes, publicación, control, información, organización de programas de formación específica sobre SIV y SIS II, ejecución de planes piloto previa petición concreta y específica de la Comisión, y seguimiento de la investigación.[650]

El Reglamento deja la puerta abierta para que en el futuro se integren al mismo otros sistemas informáticos de gran magnitud, ya sea en aplicación del Título V del Tratado de Funcionamiento de la Unión Europea (PESC), ya sea de otros sistemas informáticos de gran magnitud en el ámbito del espacio de libertad, seguridad y justicia. Ahora bien, la integración de otros sistemas requerirá siempre un mandato específico del legislador europeo.[651]

En lo que se refiere específicamente a la protección de datos personales, el Reglamento EUROSIGMA de 2011, contempla sólo una disposición al respecto en el artículo 25, que dispone: «1. La información tratada por la Agencia de conformidad con el presente Reglamento estará sujeta al Reglamento (CE) nº 45/2001 relativo a la

---

sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia»; la COM (2009) XX final, «documento de trabajo de los servicios de la Comisión que acompaña a la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece una Agencia para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia, y a la propuesta de Decisión del Consejo por la que se confieren a la Agencia creada por el Reglamento XX funciones de gestión operativa de SIS II y VIS en aplicación del Título VI del Tratado UE»; Reglamento (CE) nº 1987/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II), DO L 381 de 28.12.2006, p. 4.

[649] La Agencia será responsable de las funciones relativas a la infraestructura de comunicación a que se refieren el artículo 15, apartado 2, de la Decisión y del Reglamento SIS II, el artículo 26, apartado 2, del Reglamento VIS y el artículo 5, apartado 2, del Reglamento relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento. Además, la Agencia desempeñará funciones de formación de expertos en VIS y SIS II que incluirán formación relativa al intercambio de información suplementaria, así como el seguimiento de las actividades de investigación y la aplicación de planes piloto previa petición concreta y específica de la Comisión. Cfr. COM (2010) 93 final.

[650] Cfr. COM (2010) 93 final.

[651] Cfr. Considerandos 4, 10, 11; artículo 1.3., 6 y 8 del Reglamento Eurosigma de 2011.

protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. 2. El Consejo de Administración adoptará medidas para la aplicación del Reglamento (CE) nº 45/2001 por la Agencia, incluidas las relativas al responsable de protección de datos de la Agencia».

Cabe recordar que cada uno de los sistemas de información que se incorporar a este sistema centralizado de gestión de la información, posee normas particulares sobre protección de datos. Por tanto, se estableció que la gestión operativa de los sistemas informáticos de gran magnitud, en el espacio de libertad, seguridad y justicia que realizará esta agencia europea, no afecta a las normas específicas que regulan los principios, derechos, medidas de seguridad y otros requisitos de protección de datos aplicables a cada uno de los sistemas.[652] En consecuencia, creemos que la responsabilidad de garantizar y proteger los datos personales tratados en estos grandes sistemas de información debe recaer, en primer lugar, en el ente u órgano comunitario que proporciona o transfiere la información a esta nueva macro plataforma de gestión de datos; pero una vez transferida, debería ser la nueva agencia EUROSIGMA la que asuma la responsabilidad en el tratamiento de los datos personales bajo las condiciones y requisitos que le impone el Reglamento 45/2001. En definitiva, lo que se debe propender es una coherencia en la protección de los titulares de los datos, con el fin último de obtener un nivel de protección elevado y equivalente de los datos personales de las personas afectadas por dicho tratamiento bajo cualquier sistema de gestión de datos para la prevención y represión penal.

Otro punto importante es el referido a las autoridades de supervisión del tratamiento de datos personales. El Reglamento en su artículo 11 contempla dentro de la orgánica de la institución a un «responsable de la protección de datos», dando cumplimiento con ello a lo dispuesto en el artículo 24 Reglamento 45/2001. Por su parte, el Supervisor Europeo de Protección de Datos está facultado para ejercer todas

[652] El Reglamento hace un reenvío a las disposiciones particulares de cada uno de estos sistema en lo relativo a la regulación de la protección de datos, en los siguientes términos: «La atribución a la Agencia de la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia no debe afectar a las normas específicas aplicables a estos sistemas. Son plenamente aplicables, en particular, las normas específicas que regulan los fines, derechos de acceso, medidas de seguridad y otros requisitos de protección de datos de cada uno de los sistemas informáticos de gran magnitud cuya gestión operativa se ha confiado a la Agencia». Cfr. Considerando 14 del Reglamento n° 1077/2011; COM (2010) 93 final, p. 11.

sus funciones y competencias en relación a los tratamientos de datos personales que se realicen por parte de esta nueva institución de gestión de datos europea.[653] Por último, cabe recordar que en el caso de Eurodac, SIS y SIV, se establece una supervisión compartida entre las autoridades nacionales y el SEPD, que supervisa el tratamiento en la unidad central.[654]

Como hemos tenido oportunidad de señalar, el Reglamento 1077/2011 que crea la Agencia Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia, deja subsistente las normas específicas de cada uno de los órganos comunitario que tratan datos personales para el cumplimiento de sus fines; por ello es necesario realizar una revisión general sobre los mismos, con la finalidad de determinar el nivel de protección que se brinda a los datos personales en cada uno de estos sistemas y los mecanismos de control establecidos para garantizar el respeto al derecho fundamental a la protección de datos personales. Atendido el objeto limitado de esta tesis, centraremos nuestros análisis en tres sistemas: el Sistema de Información Schengen (SIS), El Sistema de Información de Visados (SIV), y el Sistema de Comparación de Huellas Dactilares (Eurodac).[655] Dichos sistemas ya han sido objeto

[653] Cfr. artículo 46 y 47 del Reglamento 45/2001 y Considerando 23 del Reglamento Eurosigma de 2011, p. 3. Una de las inquietudes más serias manifestadas por el SEPD sobre Agencia para la gestión operativa de sistemas informáticos a gran escala en el ámbito de la libertad, la seguridad y justicia, es el riesgo que de la desviación de uso de los datos y las consecuencias de la interoperabilidad de los sistemas. Al respecto véase el Dictamen del Supervisor Europeo de Protección de Datos «sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece una Agencia para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia, y sobre la propuesta de Decisión del Consejo por la que se asignan a la Agencia creada por el Reglamento XX las tareas relativas a la gestión del SIS II y el VIS en aplicación del título VI del Tratado UE», publicado en el DOUE n° C 70, de 19.3.2010.

[654] Con el fin de promover la buena cooperación con las autoridades nacionales, el SEPD organiza reuniones de coordinación. La aplicación de este "modelo de supervisión coordinada", también se puede aplicar a otros sistemas de TI a gran escala, como el sistema es estudio.

[655] Existen otros sistemas que también impactan en el tratamiento de datos personales con fines de prevención y represión penal, tales como Sistema de Información Aduanera (SIA) y el Sistema de Información Europeo de Antecedentes Penales (Ecris). Al respecto, véase Mónica ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, pp. 288-289; Javier ÁLVAREZ HERNANDO, *Guía práctica sobre Protección de Datos: cuestiones y formularios* (Valladolid: Lex Nova, 2011), pp. 579-580; Comisión, «Propuesta de Decisión del Consejo sobre el establecimiento del sistema de información europeo de antecedentes penales (ECRIS) en aplicación del artículo 11 de la Decisión Marco 2008/XX/JAI», accedido 7 de octubre de 2013, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0332:FIN:ES:PDF; «Protocolo establecido sobre la base del artículo K.3 del Tratado de la Unión Europea, sobre la definición del concepto de blanqueo de capitales y sobre la inclusión de información sobre matrículas de vehículos en la lista de datos del Convenio relativo a la utilización de la tecnología de la información a efectos aduaneros», accedido 7 de octubre de 2013, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:1999:091:0001:0001:ES:PDF; «Resolución del Consejo, de 13 de diciembre de 2011, sobre el futuro de la cooperación en la aplicación de la legislación

de la atención por parte de la doctrina, por tanto, nos avocaremos esencialmente a la revisión de las modificaciones introducidas por el Tratado de Lisboa en la regulación de dichas materias.

5.1. El Sistema de Información Schengen (SIS)

La libre circulación de personas en el espacio de Schengen constituye uno de los logros más importantes de la integración europea.[656] Este espacio, tiene su origen en el Acuerdo de Schengen de 1985 («Schengen I») y su Convenio de aplicación de 1990 («Schengen II») cuya finalidad era suprimir gradualmente los controles en las fronteras y establecer un régimen de libre circulación para todos los nacionales de los Estados signatarios, de los otros Estados de la Comunidad y de terceros países.[657]

El objeto principal del Convenio Schengen es la supresión gradual de los controles fronterizos de los Estados Miembros. Como contrapartida al establecimiento de un espacio de libre circulación se creó el Sistema de Información de Schengen (SIS), que permite a las autoridades asignadas por las partes contratantes, gracias a un sistema informatizado, disponer de descripciones de personas y de objetos, con ocasión de controles en las fronteras, aduanas y controles de policía.[658] Por tanto, el objetivo principal del Convenio no fue la regulación del tratamiento de datos personales, sino

---

en materia aduanera - LexUriServ.do», accedido 7 de octubre de 2013, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:005:0001:0003:ES:PDF.

[656] El derecho de libre circulación es un derecho fundamental; las condiciones de su ejercicio están definidas en el Tratado de la Unión Europea (TUE) y en el Tratado de Funcionamiento de la Unión Europea (TFUE), así como en la Directiva 2004/38/CE del Parlamento Europeo y del Consejo, de 29 de abril de 2004, relativa al derecho de los ciudadanos de la Unión y de los miembros de sus familias a circular y residir libremente en el territorio de los Estados Miembros, publicada en el DOUE n° L 158 de 30.4.2004, p. 77.

[657] El Acuerdo de Schengen, fue firmado el 14 de junio de 1985 entre Alemania, Bélgica, Francia, Luxemburgo y los Países Bajos. El Convenio de aplicación, suscrito el 19.06.1990 completa el Acuerdo y define las condiciones y las garantías de aplicación de esta libre circulación. Publicado en el DOCE n° L 239 de 22.9.2000, p. 19. El Acuerdo y el Convenio, así como las normas y acuerdos conexos conforman el «acervo de Schengen». Cabe recordar que el «espacio Schengen» comprende Estados asociados, como lo son Suiza, Islandia y Noruega, que no forman parte de la Unión Europea. Sobre el origen y desarrollo del Espacio Schengen, véase, entre otros: F. J. INDA, «Schengen: referencia en materia de coordinación policial», *Harlax: Ertzainaren lanbide aldizkaria = Revista técnica del Ertzaina* N° 11 (1995): pp. 32-93; José Manuel LUQUE GONZÁLEZ, «Schengen. Un espacio de libertad, seguridad y justicia», *Revista de derecho: División de Ciencias Jurídicas de la Universidad del Norte* N° 21 (2004): pp. 139-149; María del Carmen GUERRERO PICÓ, *El Impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal* (Thomson Civitas, 2006): pp. 120-127; Antonio RUÍZ CARRILLO, *Los datos de carácter personal. Concepto, requisitos de circulación, procedimientos y formularios* (Barcelona: Bosch, 1999): p. 109.

[658] Cfr. Título IV del Convenio de 19 de junio de 1990 de aplicación del Acuerdo de Schengen.

que ello se dio por accesión, al tener como elemento o insumo principal para el cumplimiento de sus fines el uso de los datos de las personas que ingresan al espacio Schengen.[659]

El Sistema de Información Schengen ha sufrido varios cambios respecto de su configuración original producto de varios factores, entre los que podemos señalar, el aumento del número de países que integran la Unión Europea, los acelerados avances tecnológicos en la materia y las transformaciones institucionales y jurídicas que ha traído el Tratado de Lisboa.[660]

En primer lugar, desde 1999 el acervo de Schengen pasó a estar integrado en el marco institucional y jurídico de la Unión Europea en virtud de protocolos anexos a los Tratados.[661] Luego, en el 2001, ante la limitada capacidad del originario SIS, se decidió la creación de un nuevo Sistema de Información Schengen de segunda generación (SIS II).[662] Posteriormente, en 2004, se le añadieron nuevas funciones al SIS, tales como la lucha contra el terrorismo, en particular en lo que se refiere a la posibilidad de acceso a determinados tipos de datos para facilitar la búsqueda de información a Europol y a los miembros europeos de Eurojust.[663] Después, y en la misma línea, el Tratado de Prüm, que algunos denominan Sistema Información Schengen III, estableció un sistema de intercambio de información sobre personas relacionadas con actividades terroristas, la

[659] En el mismo sentido véase Mónica ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, p. 286.
[660] Al respecto véase Rafael ARENAS GARCÍA y Joan Lluís PÉREZ FRANCESCH, "Extranjería (II) entrada en el espacio Schengen y permanencia en España", en Mª del Carmen GETE-ALONSO Y CALERA y Judith SOLÉ RESINA (Coord.), *Tratado de Derecho de la Persona Física*, Vol. 2, Cívitas, Navarra, 2013, pp. 467-536.
[661] Cfr. Tratado de Ámsterdam de 2 de octubre de 1997; el Protocolo (n° 19) sobre el acervo de Schengen integrado en el marco de la Unión Europea, p. 290; y las Declaraciones relativa al artículo 5 del Protocolo sobre el acervo de Schengen integrado en el marco de la Unión Europea, p. 352, ambas del TFUE.
[662] Cfr. El Reglamento 2424/2001, de 6 de diciembre, del Consejo, sobre el desarrollo del Sistema de Información Schengen de segunda generación (SIS sobre el desarrollo del Sistema de Información Schengen de segunda generación (SIS II), publicado en el DOCE n° L 328, de 13.12.2001; y la Decisión 2001/886/JAI, de 6 de diciembre, del Consejo, sobre el desarrollo del Sistema de Información Schengen de segunda generación (SIS II), publicada en el DOCE n° L 328, de 13.12.2001. Al respecto véase también el Dictamen de 19 de mayo de 2004, del Presidente de la Autoridad de Control Común Schengen, sobre el desarrollo del SIS II (Bruselas, 24 de mayo, SCHAC 2504/04).
[663] Cfr. Reglamento 871/2004, de 29 de abril, del Consejo, sobre la introducción de nuevas funciones para el Sistema de Información Schengen, inclusive en materia de lucha contra el terrorismo, publicado en el DOUE n° L 162, de 30.4.2004; y la Decisión 2005/451/JAI, de 13 de junio, del Consejo, por la que se fija la fecha de aplicación de determinadas disposiciones del Reglamento 871/2004, publicada en el DOUE n° L 158, de 21 de junio.

creación de bases de datos nacionales de análisis de ADN, así como la comparación de perfiles de ADN y la consulta de los datos dactiloscópicos.

En el año 2007, se estableció un nuevo Sistema de Información Schengen, que tenía por finalidad conciliar un alto nivel de seguridad en el espacio de libertad, seguridad y justicia de la Unión, con la aplicación de las disposiciones del título IV de la Tercera parte del Tratado CE relativas a la circulación de personas en dicho territorio.[664] Dado que los antiguos elementos del SIS II afectaban a diversos pilares, el marco jurídico del SIS se componía de reglamentos del primer pilar y de decisiones del tercer pilar.[665] Aunque esta distinción desapareció con la entrada en vigor del Tratado de Lisboa el 1 de diciembre de 2009, los instrumentos existentes aún reflejan la antigua estructura de pilares.[666] Actualmente, la base jurídica de toda la normativa Schengen se

[664] Cfr. Artículo 1.2. de la Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II). Esta Decisión contempla entre otros extremo, «especificar […] las categorías de datos que se introducirán en el sistema, los fines para los que se introducirán, los criterios de introducción, las autoridades autorizadas para acceder a los datos, la interconexión entre las descripciones, y otras normas sobre tratamiento de datos y protección de datos personales». Cfr. Considerando 6 de la Decisión 2007/533/JAI.

[665] El Sistema de Información de Schengen de segunda generación (SIS II) fue establecido por el Reglamento (CE) nº 1987/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, y por la Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del sistema de información de Schengen de segunda generación (SIS II), publicado en el DO n° L 381 de 28.12.2006, p. 4 y n° L 205 de 7.8.2007, p. 63.

[666] Cfr. Reglamento (CE) nº 2424/2001 del Consejo, de 6 de diciembre de 2001, sobre el desarrollo del Sistema de Información de Schengen de segunda generación (SIS II) y Decisión 2001/886/JAI del Consejo, de 6 de diciembre de 2001, sobre el desarrollo del Sistema de Información de Schengen de segunda generación (SIS II), ambas publicados en el DO n° L 328 de 13.12.2001, p. 1 y 4; Reglamento (CE) nº 1987/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II) y Reglamento (CE) nº 1986/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativo al acceso al Sistema de Información de Schengen de segunda generación (SIS II) por los servicios de los Estados Miembros competentes para la expedición de los certificados de matriculación de vehículos, ambos publicados en e DO n° L 381 de 28.12.2006, p. 1 y 4; Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II), publicado en el DO n° L 205 de 7.8.2007, p. 63.; Decisiones 2007/170/CE y 2007/171/CE de la Comisión, de 16 de marzo de 2007, por las que se establecen los requisitos de la red para el Sistema de Información de Schengen II, publicado en el DO n° L 79 de 20.3.2007, p. 20.; Reglamento (CE) nº 189/2008 del Consejo, de 18 febrero 2008, sobre los ensayos del Sistema de Información de Schengen de segunda generación (SIS II) DO n° L 57 de 1.3.2008, p. 1; Decisión 2008/173/CE del Consejo, de 18 febrero 2008, relativa a los ensayos del Sistema de Información de Schengen de segunda generación (SIS II), publicado en el DO L 57 de 1.3.2008, p. 14; Decisiones 2008/333/CE y 334/2008/JAI de la Comisión, de 4 de marzo de 2008, por la que se adopta el Manual SIRENE y otras medidas de ejecución para el Sistema de Información de Schengen de segunda generación (SIS II), publicado en el DO n° L 123 de 8.5.2008, p. 1; Reglamento (CE) nº 1104/2008 del Consejo, de 24 de octubre de 2008, sobre la migración del Sistema de Información de Schengen (SIS 1+) al Sistema de Información de Schengen de segunda generación (SIS II) y la Decisión 2008/839/JAI del Consejo, de 24 de octubre de 2008, sobre la migración del Sistema de Información de Schengen (SIS 1+) al Sistema de Información de Schengen de segunda generación (SIS II), ambas publicada en el DO n° L 299 de 8.11.2008, p. 1 y 43.

sustenta en el artículo 77, apartado 2, letra b), y el artículo 79, apartado 2, letra c), del TFUE, donde se establece que la Agencia abarcará técnicamente aspectos relativos a los controles sobre las personas en las fronteras exteriores, así como medidas en materia de residencia ilegal e inmigración ilegal, respectivamente.[667]

Otro hito en el proceso de evolución del Sistema de información Schengen está dado, como vimos en el apartado anterior, por la promulgación del Reglamento N° 1077/2011, del Parlamento Europeo y del Consejo, por el que se establece una Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia. Esta nueva agencia comunitaria pasó a administrar, entre otros sistemas, «la gestión operativa» del Sistema de Información de Schengen. Ahora bien, en lo que respecta al marco normativo aplicable a la protección de los datos personales, el Reglamento 1077/2011 hace un reenvío a las disposiciones particulares sobre la materia de cada uno de los sistema que administra, pero las actividades propias que desarrolle en el ejercicio de sus funciones quedan regidas por el Reglamento 45/2001, bajo la supervigilancia del Supervisor Europeo de Protección de Datos.

Pasamos ahora a revisar qué establecen estas disposiciones particulares del Sistema de Información Schengen en lo referido al nivel de protección y la autoridad de control a cargo del cumplimiento de la normativa sobre protección de datos personales.

Sobre el primer punto, debemos recordar que al momento de dictarse la mayor parte de la normativa sobre el Sistema de Información Schengen, no existía una norma de carácter general y supletoria que regulara el tratamiento de los datos personales en el ámbito de la cooperación policial y judicial, o en términos actuales, de la prevención y

[667] Con posterioridad al Tratado de Lisboa, la política de la Unión relativa a las fronteras exteriores ha tenido como norte «establecer una gestión integrada para garantizar un nivel elevado y uniforme de control y vigilancia, corolario indispensable de la libre circulación de personas en la Unión y componente esencial del espacio de libertad, seguridad y justicia». Con este propósito, se han establecido una serie de disposiciones comunes que fijan las normas y procedimientos de control en las fronteras exteriores. Cfr. Considerando 1 del «Reglamento (UE) no 610/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, por el que se modifica el Reglamento (CE) no 562/2006 del Parlamento Europeo y del Consejo, por el que se establece un Código comunitario de normas para el cruce de personas por las fronteras (Código de fronteras Schengen), el Convenio de aplicación del Acuerdo de Schengen, los Reglamentos del Consejo (CE) no 1683/95 y (CE) no 539/2001 y los Reglamentos del Parlamento Europeo y del Consejo (CE) no 767/2008 y (CE) no 810/2009», accedido 16 de septiembre de 2013, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:182:0001:0018:ES:PDF.

represión penal. Como se sabe, bajo la lógica de división de pilares, la Directiva 95/46/CE excluía explícitamente de su ámbito de aplicación dichos ámbitos. Al no existir una norma similar en el antiguo tercer pilar, toda normativa que se dictara en éste ámbito y que contemplara el tratamiento de datos personales, tenía que incorporar un conjunto de disposiciones sobre la materia. Es por ello que toda la normativa Schengen, desde los primeros Acuerdos y Convenios, pasando por los Reglamentos y Directivas, contemplan un conjunto más o menos sistematizado y homogenizado de normas sobre tratamiento de datos personales. Para determinar el nivel de protección que se debía brindar en el tratamiento de los datos personales, dicha normativa, se remitía a los principios del Consejo de Europa en la materia, esto es, Convenio n° 108 del Consejo de Europa de 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, la Recomendación R (87) 15 de 17 de septiembre de 1987 del Comité de Ministros del Consejo de Europa, dirigida a regular la utilización de datos de carácter personal en el sector de la policía y sus modificaciones posteriores.[668]

En lo que se refiere a la autoridad de control a cargo de supervisar el cumplimiento de la normativa del Sistema de Información Schengen, podemos indicar que existe una concurrencia de autoridades competentes, que determinan su ámbito de acción en base, esencialmente, al lugar de origen y de tratamiento del dato personal. Así, se establece que las autoridades nacionales de control supervisen la legalidad del tratamiento de datos por los Estados Miembros, mientras que el Supervisor Europeo de Protección de Datos supervisa las actividades de las instituciones y los organismos comunitarios en relación con el tratamiento de datos personales.[669] En la misma línea, se estableció que las disposiciones del Convenio de 26 de julio de 1995, por el que se crea una Oficina Europea de Policía («el Convenio Europol»), que se refieren a la protección

[668] Cfr. Artículo 38 del Acuerdo de Schengen; Capítulo III, del Título IV (artículos 92 y ss.) y V (artículo 122-130) del Convenio de aplicación y artículo 57 de la Decisión 2007/633/JAI. En éste último cuerpo normativo, queda de manifiesta la voluntad de la Comisión de aplicar las normas de la futura Decisión Marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, que debía aprobarse antes de fin de 2006 (se aprobó en 2008) y aplicarse a los datos personales que se tratan en el marco del SIS II, así como a los datos relacionados con el intercambio de información complementaria de conformidad la presente Decisión Schengen. Cfr. Considerando 21 de la decisión 2007/533/JAI.

[669] Cfr. Considerando 24 de la Decisión 2007/533/JAI. Al respecto, el artículo 61.1. de ésta Decisión dispone que «El Supervisor Europeo de Protección de Datos controlará que las actividades de tratamiento de datos personales de la Autoridad de Gestión sean conformes a la presente Decisión. En consecuencia, serán de aplicación las disposiciones sobre funciones y competencias del Supervisor Europeo de Datos previstas en los artículos 46 y 47 del Reglamento (CE) no 45/2001».

de datos personales, son de aplicación al tratamiento de datos del SIS II por parte de Europol, incluidas la competencia de la Autoridad Común de Control establecida por el Convenio Europol de vigilar la actividad de Europol y la responsabilidad en caso de tratamiento ilícito o incorrecto de datos por parte de ésta institución.[670] Lo mismo ocurre con las disposiciones de la Decisión 2002/187/JAI del Consejo de 28 de febrero de 2002 por la que se crea Eurojust, para reforzar la lucha contra las formas graves de delincuencia referidas a la protección de datos personales, y que son de aplicación al tratamiento de datos del SIS II por parte de Eurojust, incluidas la competencia de la Autoridad Común de Control establecida por dicha Decisión de controlar las actividades de Eurojust y la responsabilidad por el tratamiento no autorizado o incorrecto de datos personales por parte de Eurojust.[671]

5.2. El Sistema de Información de Visados (SIV)

La idea de crear un sistema de información común para la identificación de los visados se remonta al Consejo Europeo de Sevilla de 2002.[672] No obstante, la materialización normativa del Sistema de Información de Visados (en adelante, SIV) se produjo por medio de la Decisión 2004/512/CE del Consejo, de 8 de junio de 2004.[673] A diferencia del SIS II, el SIV se estableció en el marco del antiguo primer pilar. No obstante, se adoptó un instrumento SIV del tercer pilar para que los servicios policiales designados pudieran acceder al sistema a fin de efectuar consultas relacionadas con la comisión de determinadas infracciones.

Con posterioridad a la adopción de la Decisión de 2004, se han adoptado una serie de Decisiones y Reglamentos sobre la materia, entre los que destacan: la Decisión de la Comisión 2006/752/CE, de 3 de noviembre de 2006, por la que se determinan las localizaciones del Sistema de Información de Visados durante la fase de desarrollo[674]; la Decisión de la Comisión 2006/648/CE, de 22 de septiembre de 2006, por la que se establecen las especificaciones técnicas de las normas sobre los identificadores

[670] Cfr. Considerando 26 de la Decisión 2007/533/JAI.
[671] Cfr. Considerando 27 de la Decisión 2007/533/JAI.
[672] Cfr. Conclusiones de la Presidencia del Consejo Europeo de Sevilla (21 y 22 de junio de 2002), p. 8, accedido 23 de septiembre de 2013, http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/es/ec/72639.pdf.
[673] Publicado en el DO n° L 213 de 15.6.2004, p. 5. Sobre el Sistema de Información de Visado, véase
[674] Publicado en el DO n° L 305 de 4.11.2006, p. 13.

biométricos en relación con el Sistema de Información de Visados[675]; la Decisión de la Comisión 2008/602/CE, de 17 de junio de 2008, por la que se establecen la arquitectura física y las características de las interfaces nacionales y de la infraestructura de comunicación entre el Sistema Central de Información de Visados y las interfaces nacionales para la fase de desarrollo[676]; el Reglamento (CE) nº 767/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre el Sistema de Información de Visados (SIV) y el intercambio de datos sobre visados de corta duración entre los Estados Miembros (Reglamento VIS)[677]; la Decisión 2008/633/JAI del Consejo, de 23 de junio de 2008, sobre el acceso para consultar el Sistema de Información de Visados (SIV) por las autoridades designadas de los Estados Miembros y por Europol, con fines de prevención, detección e investigación de delitos de terrorismo y otros delitos graves[678]; el Reglamento (CE) nº 81/2009 del Parlamento Europeo y del Consejo, de 14 de enero de 2009, por el que se modifica el Reglamento (CE) nº 562/2006 en lo relativo al Sistema de Información de Visados (SIV) en el marco del Código de Fronteras Schengen[679]; y el Reglamento nº 977/2011 de la Comisión, de 3 de octubre de 2011, que modifica el Reglamento por el que se establece el Código de Visados.[680]

Entre las múltiples funciones del Sistema de Información de Visado, se encuentran la posibilidad de que los Consulados y otras autoridades competentes de los Estados Miembros pueden intercambiar datos sobre visados con el fin de agilizar el procedimiento de su solicitud, impedir la búsqueda de visados de conveniencia, contribuir a la lucha contra el fraude, facilitar los controles en los puntos de paso de las fronteras exteriores y en los Estados Miembros, asistir en la identificación de nacionales de terceros países, facilitar la aplicación del Reglamento de Dublín[681] y contribuir a

[675] Publicado en el DO n° L 267 de 27.9.2006, p. 41.
[676] Publicado en el DO n° L 194 de 23.7.2008, p. 3.
[677] Publicado en el DO n° L 218 de 13.8.2008, p. 60.
[678] Publicado en el DO n° L 218 de 13.8.2008, p. 129.
[679] Publicado en el DO n°L 35 de 4.2.2009, p.56
[680] Publicado en el DO n° L 258 de 4.10.2011, p. 9.
[681] Reglamento (CE) n° 343/2003 del Consejo, de 18 de febrero de 2003, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de asilo presentada en uno de los Estados Miembros por un nacional de un tercer país. Publicado en el DO n° L 50 de 25.2.2003, p. 1/10.

prevenir las amenazas contra la seguridad interior en cada uno de los Estados Miembros.[682]

El Reglamento 767/2008 (Reglamento SIV) dispone que la Comisión será responsable durante un período transitorio de la gestión operativa del VIS. Transcurrido este período transitorio, una Autoridad de Gestión será responsable de la gestión operativa del VIS central y de las interfaces nacionales, así como de determinados aspectos de la infraestructura de comunicación. Actualmente, la Autoridad de Gestión a cargo del VIS es la Agencia Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia.[683] Dicha Agencia, tiene su base jurídica en el artículo 77, apartado 2, letra a), del TFUE, y tiene por finalidad apoya técnicamente los procedimientos de expedición de visados por los Estados Miembros.[684]

5.3. El Sistema de Comparación de Huellas Dactilares (Eurodac)

El Sistema de Comparación de Huellas Dactilares (en adelante, Eurodac) es un sistema de tecnología de la información a escala de la Unión, que busca determinar por medio de un control biométrico (impresiones dactilares) la identidad exacta de las personas. Como la mayoría de los instrumentos normativos y sistemas de información analizados en este apartado, encuentra su origen en un Acuerdo internacional (Convenio de Dublín)[685] suscrito por algunos países de la Unión con el objeto de determinar la identidad exacta de personas que solicitaban asilo o intentaban cruzar ilegalmente las fronteras exteriores de los Estados suscriptores.[686] No obstante, con posterioridad se le han ido agregando otras finalidades, vinculadas principalmente a la prevención y

[682] Cfr. COM (2010) 93 final, «Propuesta modificada de reglamento (ue) nº…/…del Parlamento Europeo y del Consejo por el que se crea una Agencia para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia», p. 8.
[683] Se espera que el futuro Sistema de Información de Visados, haga frente a 20 millones de nuevos registros por año. Cfr. https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/ITsystems [consulta 5.9.2013].
[684] Cfr. COM (2010) 93 final, p. 11.
[685] Publicado en el DO nº L 316 de 15.12.2000, p. 1. El Convenio de Dublín fue sustituido por un instrumento legislativo de la Unión, el Reglamento (CE) n° 343/2003 del Consejo, de 18 de febrero de 2003, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de asilo presentada en uno de los Estados Miembros por un nacional de un tercer país.
[686] Convenio de Dublín.

represión penal, entre las que destacan, la lucha contra los delitos de terrorismo y otros delitos graves bajo el principio de disponibilidad.[687]

Eurodac, pasa a formar parte de la legislación europea, dentro del antiguo primer pilar comunitario, a través del Reglamento (CE) nº 2725/2000 del Consejo, de 11 de diciembre de 2000.[688] Posteriormente, se dictó el Reglamento (CE) n° 407/2002 del Consejo, de 28 de febrero de 2002, por el que se establecen determinadas normas de desarrollo del Reglamento (CE) n° 2725/2000 relativo a la creación del sistema Eurodac para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín.[689]

El diseño original de Eurodac contemplaba una «Unidad Central» encargada de gestionar la base central informatizada de datos dactiloscópicos y una «Infraestructura de Comunicación» que permitía la transmisión y comparación de los datos dactiloscópicos entre los Estados Miembros y el Sistema Central. Ahora bien, con la creación de la Agencia Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia, la administración operativa del Sistema Eurodac pasó a ser realizada por esta nueva entidad europea.[690] La labor desarrollada por Eurosigma en estos casos es de apoyo técnico en el proceso de

[687] Una clara manifestación de estas nuevas dimensiones otorgadas a este sistema de información la encontramos en el Reglamento Eurodac, de 26 de junio de 2013, donde se señala que «La información que contiene Eurodac es necesaria a efectos de prevención, detección o investigación de los delitos de terrorismo como se contempla en la Decisión Marco del Consejo 2002/475/JAI, de 13 de junio de 2002, sobre la lucha contra el terrorismo o de otros delitos graves como se contempla en la Decisión Marco del Consejo 2002/584/JAI, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados Miembros. Por lo tanto, los datos de Eurodac deben estar disponibles, con sujeción a las condiciones establecidas en el presente Reglamento, para su comparación por las autoridades designadas de los Estados Miembros y la Oficina Europea de Policía (Europol)». Cfr. Considerando 8 del Reglamento (UE) N° 603/2013 del Parlamento y del Consejo, de 26 de junio de 2013, p. 2.

[688] Reglamento relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín, publicado en el DOCE nº L 316 de 15.12.2000, p. 1. Al respecto véase Jonathan P. AUS, «Eurodac: A Solution Looking for a Problem?», *European integration online papers (EIoP)* Nº 10 (21 de julio de 2006): pp. 1-26; Irene CLARO QUINTÁNS, «El sistema "Eurodac" y la identificación de los solicitantes de asilo en la Unión Europea», en *El día de Europa: las transformaciones de la Unión Europea : la ampliación y la convención europea : actas de las II jornadas en conmemoración del Día de Europa de la Universidad Pontificia Comillas de Madrid, 8 y 9 de mayo de 2003*, ed. María Susana de Tomás Morales, Christine Heller del Riego, y María Esther Vaquero Lafuente (Madrid: Universidad Pontificia Comillas, 2004): pp. 215-228; Mónica ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa* (Valencia: Tirant lo Blanch, 2006): pp. 291 y 292. .

[689] Publicado en el DO nº L 62 de 5.3.2002, p. 1.

[690] Cfr. Considerando 3 del Reglamento (UE) Nº 1077/2011 del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, por el que se establece una Agencia Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia.

determinación del Estado Miembro responsable del examen de una solicitud de asilo presentada por un nacional de un tercer país en un Estado Miembro.[691]

En lo referido a la legislación aplicable en materia de protección de datos personales, lo primero es consignar que los Reglamentos que se han dictado en la materia contienen disposiciones específicas sobre protección de datos. Así por ejemplo, el Reglamento del año 2000 regula, entre otros extremos, la toma, transmisión y comparación de los datos dactiloscópicos, así como su registro y conservación tanto en los casos de solicitud de asilo como en casos de extranjeros interceptados en un cruce irregular de la frontera (Capítulos II y III). Además, reconoce la posibilidad de un bloqueo de los datos para el caso de refugiados reconocidos (Capítulo V) y regula la utilización de los datos y su protección, reconociendo los derechos de acceso, rectificación y cancelación de los datos registrados en Eurodac (Capítulo VI).

Ahora bien, antes de determinar el marco normativo supletorio aplicable al tratamiento de datos personales, cabe recordar que en su origen Eurodac se creó para facilitar la aplicación del Convenio de Dublín, es decir, dentro del antiguo primer pilar comunitario. Por tanto, en principio, le son plenamente aplicables la normativa general establecidas en las Directivas sobre protección de datos, y en particular, la Directiva 95/46/CE.[692] No obstante, el fin original de Eurodac ha ido cambiando con el tiempo al comprobarse la utilidad del sistema para la prevención, detección o investigación de los delitos de terrorismo o de otros delitos graves, sobre todo después de los fatídicos atentados terrorista de Madrid, Londres y Nueva York.

---

[691] Cfr. artículo 78, apartado 2, letra e), del TFUE); y la Propuesta modificada de reglamento (ue) nº …/…del Parlamento Europeo y del Consejo por el que se crea una Agencia para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia (presentada por la Comisión de conformidad con el artículo 293, apartado 2, del Tratado de Funcionamiento de la Unión Europea), COM (2010) 93 final, p. 12.

[692] Cfr. Considerando 38 del «Reglamento (UE) no 603/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativo a la creación del sistema Eurodac para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (UE) no 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados Miembros por un nacional de un tercer país o un apátrida, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados Miembros y Europol a efectos de aplicación de la ley, y por el que se modifica el Reglamento (UE) no 1077/2011, por el que se crea una Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia - LexUriServ.do», accedido 3 de septiembre de 2013, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:180:0001:0030:ES:PDF.

En estos casos, vinculados al antiguo tercer pilar comunitario, las autoridades designadas o verificadoras de los Estados Miembros en la gestión de Eurodac deben garantizar un nivel de protección de los datos personales con arreglo al Derecho nacional, el que a su vez, debe ofrecer un nivel mínimo de protección conforme con 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.[693] No debe olvidarse, también, que el Reglamento (CE) n° 45/2001[694], se aplican al tratamiento de datos personales llevado a cabo por las instituciones, organismos, oficinas y agencias de la Unión, lo que incluye las actividades desarrolladas por Eurodac[695]

En cuanto a las autoridades encargadas de controlar y fiscalizar el respeto a las normas sobre protección de datos, nuevamente hay que realizar una distinción. Las autoridades nacionales de control supervisan la legalidad del tratamiento de datos personales realizados por las autoridades competentes de los Estados Miembros, destinadas a gestionar la utilización de huellas dactilares. Por su parte, el Supervisor Europeo de Protección de Datos es la autoridad competente, según lo dispuesto en el Reglamento (CE) n° 45/2001, para supervisar las actividades de Eurodac en relación con el tratamiento de datos personales.[696]

---

[693] Ibídem, considerando 39. Sobre la Decisión Marco 2008/977/JAI, véase *supra*, apartado1 de este capítulo. Sobre este punto el SEPD ha sido crítico, indicando en uno de sus Dictámenes que «la necesidad de claridad sobre el modo en que las disposiciones de la propuesta que especifican determinadas obligaciones y datos en materia de protección de datos hacen referencia tanto a la Decisión Marco 2008/977/JAI como a la Decisión 2009/371/JAI del Consejo. Cfr. *Resumen ejecutivo informe anual SEPD 2012*, sección 4.

[694] Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos de la Comunidad y a la libre circulación de estos datos, publicado en el DOCE n° DO L 8 de 12.1.2001, p. 1.

[695] Es importante destacar el cambio de percepción en relación a la normativa sobre protección de datos, de ser considerado un lastre para garantizar la seguridad de los ciudadanos de la Unión, se ha pasado a tomar conciencia de la importancia del mismo, para el buen funcionamiento de las propias instituciones y sistemas de la Unión encargadas de garantizar la prevención y represión penal. En este sentido, el Reglamento Eurodac de 2013, señala que «…es preciso aclarar determinados puntos relativos a la responsabilidad derivada del tratamiento de los datos y de la supervisión de la protección de los datos, teniendo en cuenta que la protección de datos es un factor clave para el buen funcionamiento de Eurodac y que la seguridad de los datos, la elevada calidad técnica y la legalidad de las consultas son esenciales para garantizar el funcionamiento correcto y libre de contratiempos de Eurodac y para facilitar la aplicación del Reglamento (UE) n o 604/2013». Cfr. Considerando 43.

[696] Considerando 45 del Reglamento Eurodac de 2013. Al respecto, cabe tener presente algunas reflexiones del SEPD sobre el uso de los datos personales contenidos en EURODAC, con fines de prevención y represión penal. Partiendo de la base de que acceder a los datos EURODAC a efectos de aplicación de la ley ha sido objeto de un extenso debate en la Comisión, el Consejo y el Parlamento Europeo, entiende, que «la disponibilidad de una base de datos con impresiones dactilares puede resultar un instrumento útil complementario en la lucha contra la delincuencia. Sin embargo, el SEPD recuerda

asimismo que dicho acceso a EURODAC tiene un grave impacto sobre la protección de los datos personales de las personas cuyos datos están almacenados en el sistema EURODAC. Para poder ser considerada válida, la necesidad de dicho acceso debe apoyarse en elementos claros e indiscutibles, y debe quedar demostrada la proporcionalidad del tratamiento. Esto resulta aún más necesario si se produce una intromisión en los derechos de las personas que constituyen un grupo vulnerable necesitado de protección, tal como se prevé en la propuesta». Cfr. «Resumen del Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta modificada de Reglamento del Parlamento Europeo y del Consejo relativo a la creación del sistema EURODAC para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (UE) no […/…]», p. 1. Disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:028:0003:0005:ES:PDF. [consultado el 26.9.2013]

TERCERA PARTE

TRATAMIENTO DE LOS DATOS PERSONALES EN EL ÁMBITO DE LA PREVENCIÓN Y REPRESIÓN PENAL EUROPEA

CAPÍTULO SEPTIMO

ANALISIS CRÍTICO DE ALGUNOS ASPECTOS SUBJETIVOS DEL TRATAMIENTO DE DATOS CON FINES DE PREVENCIÓN Y REPRESIÓN PENAL

SUMARIO: INTRODUCCIÓN. 1. INTERESADOS (titulares de los datos); 1.1. Personas físicas (naturales); 1.1.1. Personas relacionadas directamente con una infracción penal; 1.1.2. Terceros relacionados indirectamente con una infracción penal; 1.1.3. Terceros sin relación con una infracción penal; 1.1.4.Menores vinculados a infracciones penales; 1.2. Personas jurídicas (morales). 2. LOS DERECHOS DE LOS TITULARES; 2.1. Derecho a la información; 2.2. Derecho de acceso; 2.3. Derecho de rectificación; 2.4. Derecho de oposición, supresión (cancelación) y bloqueo; 2.5. Derecho a presentar un recurso; 2.6. Derecho a ser indemnizado; 3. LOS LÍMITES Y EXCEPCIONES AL EJERCICIO DE LOS DERECHOS; 3.1. Consideraciones preliminares; 3.2. Regulaciones de los límites y excepciones en el tratamiento de datos con fines de prevención y represión penal.

INTRODUCCIÓN

El presente capítulo se destina al análisis del ámbito de aplicación subjetivo del tratamiento de datos personales en materia de cooperación policial y judicial penal. Para ello, hemos dividido el capítulo en dos partes, una destinada a revisar las principales modificaciones que se introducen en la regulación de los titulares de los datos (interesados); y la otra, al estudio de los derechos que se consagran en favor de interesados en la actual y futura legislaciones que rige la materia.

La primera parte inicia con una referencia a la evolución y delimitación actual de las diferentes denominaciones que se refieren al sujeto activo de la protección de los datos personales. Luego, se realiza una distinción entre la regulación de la materia entre personas físicas y jurídicas, poniendo el acento en las diferentes categorías de interesados que se ven involucrados en el tratamiento de datos personales con fines de prevención y represión penal. En este último punto, resulta particularmente sensible el tratamiento de datos personales de las personas que no tienen ningún tipo de relación

con infracción penal, así como la situación de los menores de edad cuyos datos son tratados con fines de prevención o represión penal.

En la segunda parte, veremos de qué forma las facultades o derechos que son inherentes al derecho fundamental a la protección de datos personales están presentes en el caso que el tratamiento esté destinado a la prevención y represión penal. Partiendo desde la legislación del Consejo de Europa hasta las disposiciones particulares que recoge la Decisión Marco 2008/977/JAI, podremos ponderar el aporte real de las modificaciones que pretende introducir en la materia la propuesta de Directiva COM (2012) 10 final de 25.1.2012. Por último, revisaremos el alcance y condiciones que tienen las injerencias (límites y excepciones) a los derechos reconocidos para custodiar la autodeterminación informativa.

1. INTERESADOS (titulares de los datos)

Los términos que se utilizan para referir a los individuos cuyos datos son objeto de tratamiento han cambiado sustancialmente. Las primeras regulaciones se referían al titular de los datos como la «persona concernida»[697] o «sujeto de los datos».[698] A partir de la Directiva 95/46/CE, se empieza a hablar de «interesado»[699], «afectado» e incluso «usuario», en el caso de las comunicaciones electrónicas, conceptos que se han mantenido en las regulaciones posteriores, incluido el ámbito de la cooperación policial y judicial. Así, la Decisión Marco 2008/977/JAI alude al interesado al definir qué se debe entender por datos personales.[700] Más explícita y clara nos parece la modificación que introduce al respecto tanto la propuesta de Directiva en el ámbito de la prevención y represión penal, como la propuesta de Reglamento General sobre Protección de Datos, ambas de 2012, ya que distinguen conceptualmente «datos personales» de «interesado». Éste último lo define como «toda persona física identificada o que pueda ser identificada, directa o indirectamente, por medios que puedan ser utilizados razonablemente por el responsable del tratamiento o por cualquier otra persona física o

[697] Artículo 2 b) del Convenio 108 del Consejo de Europa de 1981.
[698] Directrices OCDE sobre *protección de la privacidad y el flujo transfronterizo de datos personales* de 1980.
[699] Artículo 2 a) de la Directiva 95/46/CE.
[700] El artículo 2. a) de la Decisión Marco, define *datos personales*, «como toda información sobre una persona física identificada o identificable ("el interesado")».

jurídica, en particular mediante un número de identificación, datos de localización, identificador en línea o uno o varios elementos específicos de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona»; y datos personales, como «toda información relativa a un interesado».[701] De esta forma se clarifica quién es el "sujeto" de la protección (interesado) y cuál es el "objeto" de la misma (datos personales).

Para determinar si una persona física es «identificable», se ha establecido como criterio general que deben tenerse en cuenta todos los medios que, razonablemente, pudiera utilizar el responsable del tratamiento o cualquier otro individuo para identificar a una persona.[702] Así, por ejemplo, se considerarán datos personales el nombre, el número nacional de identificación, como también cualquier otro elemento característico de la identidad física, fisiológica, psíquica, económica, cultural o social de una persona, tales como la voz, la imagen, las huellas dactilares o la información genética.[703] Los datos convertidos en «anónimos», de forma que el interesado a quien se refieren ya no resulte identificable, quedan excluidos de la protección de datos personales.[704]

En los siguientes apartados procederemos a estudiar cada uno de estos diferentes interesados, pero partiendo de una distinción mayor entre personas naturales o físicas y personas jurídicas o morales, y la discusión sobre la posibilidad de inclusión o no de éstas últimas como sujeto de protección.

1.1. Personas físicas (naturales)

Es indiscutible que los interesados o titulares de los derechos a la protección de datos son, en primer lugar, las personas físicas. Ahora bien, atendida la naturaleza de las actividades que se desarrollan en relación a la prevención y represión penal, los datos

[701] Cfr. artículos 3.1 y 3.2 de la propuesta de Directiva COM (2012) 10 final, y artículos 4.1 y 4.2 de la propuesta de Reglamento COM (2012) 11 final, p. 26.
[702] Cfr. Considerando 26 y artículo 2 a) de la Directiva 95/46/CE; artículo 2 a) de la Decisión Marco 2008/977/JAI; considerando 23 de la propuesta de Reglamento general de protección de datos; y considerando 16 de la propuesta de Directiva sobre prevención y represión penal.
[703] Sobre cuando se entiende identificada o identificable una persona, véase Javier APARICIO SALOM, *Estudio sobre la ley orgánica de protección de datos de carácter personal*, 3º ed. (Pamplona: Aranzadi, 2009), pp. 54–55.; Mónica ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa* (Valencia: Tirant lo Blanch, 2006), pp. 302-303.
[704] Ídem.

que se tratan pueden referirse a diversas «categorías de interesados». Así, la legitimación para el tratamiento de los datos de una persona puede deberse a que ésta sea sospechosa o haya participado en calidad de autor, cómplice o encubridor de una infracción penal. Pero también puede ocurrir en este tipo de actividad se traten datos de las víctimas, e incluso de terceros, v.g. los testigos. Parece lógica, entonces, la necesidad distinguir el tipo de tratamiento en función de la calidad o condición que ocupa la persona en relación a un eventual hecho ilícito investigado. No obstante, hasta ahora ni la Directiva 95/46/CE ni la Decisión Marco 2008/977/JAI, contemplaban estas distinciones.[705]

Esta situación podría cambiar parcialmente si se aprueba la propuesta de Directiva de 2012, ya que ésta en su artículo 5 introduce una distinción entre cinco categorías diferentes de interesados, a saber: a) personas respecto de las cuales existan motivos fundados para presumir que han cometido o van a cometer una infracción penal; b) personas condenadas por una infracción penal; c) víctimas de una infracción penal o personas respecto de las cuales existan motivos fundados para presumir que pueden ser víctimas de una infracción penal; d) terceras partes involucradas en una infracción penal como, por ejemplo, personas que puedan ser citadas para testificar en investigaciones relacionadas con infracciones penales o procedimientos penales ulteriores, o personas que puedan facilitar información sobre infracciones penales, o personas de contacto o asociados de una de las personas mencionadas en las letras a) y b); y e) personas que no entren dentro de ninguna de las categorías contempladas más arriba.[706] Está disposición está inspirada en la Recomendación (87) 15 del Consejo de

[705] La propuesta original de la Comisión sobre la Decisión Marco en el ámbito de la protección de datos en la cooperación policial y judicial, sí contenía una distinción entre los diversos tipos de interesados vinculados a investigar o reprimir infracciones penales. Cfr. COM (2005) 475 final.

[706] En la propuesta de Directiva que pretende reemplazar la Decisión Marco 2008/977/JAI, se refuerza la idea de distinguir entre las diferentes categorías de interesados, cuyos datos son tratados con fines de prevención o represión penal. Específicamente, el considerando 23 de la misma señala: «Es inherente al tratamiento de datos personales en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial que se traten datos personales relativos a diferentes categorías de interesados. Por tanto, en la medida de lo posible, se debe distinguir claramente entre los datos personales de diferentes categorías de interesados tales como los sospechosos, los condenados por una infracción penal, las víctimas y terceros, como los testigos, las personas que posean información o contactos útiles y los cómplices de sospechosos y delincuentes condenados». Cfr. COM (2012) 10 final, p. 18. A nuestro juicio estas categorías se podrían haber reducido a tres: personas que hayan sido condenadas o sean sospechosas de tener algún grado de participación en la comisión de un ilícito; personas que sean víctimas o supuestas víctimas de algún delito; y terceros no vinculados a ningunas de las categorías anteriores. Respecto de éstas últimas los grados de exigencia para autorizar su tratamiento de sus datos deben ser mayor, ya que la legitimidad para autorizar dicho tratamiento disminuye en la medida que el interesado no ha tenido participación alguna en los hechos.

Europa, así como en las normas que regulan Europol y Eurojust.[707] De acuerdo con el considerando 23 de la propuesta de Directiva, tal distinción es inherente al tratamiento de datos personales en el ámbito de la cooperación judicial en materia penal y la cooperación policial. Además, dicha distinción es también necesaria para garantizar una correcta aplicación de los principios relativos al tratamiento de datos personales, tal como se define en el artículo 4 de la propuesta.[708]

Para realizar nuestro análisis hemos reagrupado las categorías de interesados señaladas en el artículo 5 de la propuesta de Directiva en personas relacionadas directamente o indirectamente con la comisión de un delito; y otros terceros no vinculados a ningunas de las categorías anteriores.[709]

1.1.1. Personas relacionadas directamente con una infracción penal

La primera categoría de interesado, cuyo tratamiento de datos está autorizada por la propuesta de Directiva, se refiere a las personas relacionadas directamente con un hecho delictivo, ya sea que existan motivos fundados para presumir que ha cometido o van a cometer una infracción penal (artículo 5.a), o ya sea personas condenadas por una infracción penal (artículo 5.b). En estos casos hablamos del "sujeto activo" del presunto hecho delictivo, por lo que en principio queda clara la legitimación para el tratamiento de los datos personales de aquellas personas. No obstante, el hecho de participar en la comisión de un ilícito o de ser sospechoso del mismo, no exime a las autoridades encargadas de la persecución del mismo y del irrestricto cumplimiento y respeto de todas las garantías que emanan de los instrumentos jurídicos supranacionales y nacionales en materia de derechos fundamentales. Ahora bien, lo que distinguiría al derecho fundamental a la protección de datos personales del resto de los derechos

[707] Cfr. Artículo 14 de la Decisión 2009/371/JAI por la que se crea la Oficina Europea de Policía (Europol); artículo 15 de la Decisión 2009/426/JAI por la que se refuerza Eurojust; y COM (2012) 10 final, p. 8.

[708] En el mismo sentido, véase el Dictamen 01/2013, de 26.02.2013, del Grupo de Trabajo del Artículo 29, contiene los aportes del Grupo de consulta a los debates sobre el proyecto de Directiva de Protección de Datos de Justicia Penal. Disponible en *http://ec.europa.eu/justice/data-protection/index_en.htm* 00379/13/EN WP 201, p. 2.

[709] La necesidad de distinguir entre el procesamiento de datos de personas no sospechosas de las relacionadas con la comisión de un ilícito, ya fue advertida por la Autoridades Europeas de Protección de Datos en 2005. Cfr. Documento sobre *aplicación de la ley y de intercambio de información en la Unión Europea*, aprobada en la Conferencia de Primavera de las Autoridades Europeas de Protección de Datos, Cracovia (Polonia), 25 y 26 de abril de 2005.

fundamentales, cuando estamos ante un proceso penal, sería que la posible vulneración del primero se puede hacer valer, en la mayoría de las ocasiones, ante la correspondiente autoridad o agencia encargada de proteger los datos personales. Así entendido, el derecho a la protección de datos personales no forma parte del conjunto de principios y derechos del proceso penal, sino de un sistema paralelo de protección que garantiza el poder de disposición del imputado sobre sus datos personales, y el uso racional de las bases de datos que los contienen por parte de los entes persecutores.[710]

Por otra parte, la propuesta de Directiva autoriza también el tratamiento de los datos personales de las víctimas o presuntas víctimas de la comisión de un ilícito (artículo 5.c). Al respecto, cabe tener presente que la necesidad de reforzar los derechos de las víctimas de la delincuencia, y garantizar que quede cubierta su necesidad de protección, apoyo y acceso a la justicia, es uno de los objetivos políticos declarados en Programa de Estocolmo y su plan de acción[711], y ha pasado a constituir una prioridad estratégica para la consolidación del espacio de libertad, seguridad y justicia en la Unión Europea.[712] En esta línea, se pretende sustituir a la Decisión Marco 2001/220/JAI del Consejo, relativa al estatuto de la víctima en el proceso penal,[713] por una nueva Directiva que establezca normas mínimas comunes sobre los derechos, el apoyo y la protección de las víctimas de delitos.[714] Al respecto el SEPD en su dictamen de febrero de 2012, propone como ideas para mejorar o reforzar la protección a la víctima, entre otras: incluir una disposición general sobre la protección de la intimidad y los datos personales, que establezca que los Estados Miembros garantizarán, en la medida de lo posible, la protección de la vida privada y familiar de las víctimas, desde el primer contacto con las autoridades oficiales durante cualquier proceso penal o después del mismo, así como también permitir que las autoridades judiciales puedan dictar medidas

[710] Al respecto, véase María Ángeles GUTIERREZ ZARZA, «La protección de datos personales como derecho fundamental del imputado, ¿también en el ámbito del proceso penal?», *La ley penal: revista de derecho penal, procesal y penitenciario* Nº 71 (2010): pp. 1 y ss.
[711] Cfr. DOUE n° C 115 de 2010, p. 1; COM (2010) 171.Sobre el Programa de Estocolmo, véase *supra* apartado 1.3 del capítulo quinto de este trabajo.
[712] Al respecto, véase la Comunicación de la Comisión «Refuerzo de los derechos de las víctimas en la UE», COM (2011) 274 final, de 18.5.2011, p. 2.
[713] Publicada en el DO n° L 82 de 22.3.2001, p. 1.
[714] El 18 de mayo de 2011, la Comisión adoptó un paquete de medidas legislativas sobre la protección de las víctimas de la delincuencia. El paquete legislativo incluye una propuesta de Directiva por la que se establecen normas mínimas sobre los derechos, el apoyo y la protección de las víctimas de delitos (en adelante, la «Directiva propuesta») y una propuesta de Reglamento relativo al reconocimiento mutuo de medidas de protección en materia civil (en adelante, el «Reglamento propuesto»). Ambas propuestas vienen acompañadas por una Comunicación de la Comisión sobre el refuerzo de los derechos de las víctimas en la UE. Cfr. COM (2011) 275; COM (2011) 276; y COM (2011) 274, respectivamente.

de protección «durante la investigación penal»; especificar una lista de medidas mínimas que las autoridades judiciales podrán adoptar para proteger la intimidad y las imágenes fotográficas de las víctimas y sus familiares; establecer que los Estados exijan a todas las autoridades que estén en contacto con las víctimas, que adopten normas claras mediante las cuales se comprometan a no difundir a terceros la información que les ha sido comunicada por la víctima o que concierna a ésta; a establecer los requisitos para ofrecer a las víctimas información relativa al posterior tratamiento de sus datos personales; a aclarar el alcance del requisito de confidencialidad de los servicios de apoyo a las víctimas, y a especificar que la víctima debería tener el derecho de denegar la difusión de las comunicaciones confidenciales mantenidas con un proveedor de servicios de apoyo en cualquier procedimiento judicial o administrativo y que, en principio, dichas comunicaciones únicamente puedan ser difundidas por un tercero con su consentimiento.[715] En definitiva, lo que se busca con todas estas medidas es que la ley reconozca las diferencias que se deben realizar entre el tratamiento de los datos personales de personas condenadas y de las víctimas de un delito, sobre todo en las bases de datos creadas con fines preventivos o de represión de futuros hechos delictuales.[716]

1.1.2. Terceros relacionados indirectamente con una infracción penal

La propuesta de Directiva sobre tratamiento de datos personales en el ámbito de la prevención y represión penal, también contempla el tratamiento de datos personales de terceras personas no involucradas directamente en los hechos, tales como los testigos, informantes o personas de contacto (artículo 5.d). Es evidente en relación a dichos interesados, que la Directiva debería dejar claro que las limitaciones y garantías adicionales que se apliquen a las víctimas se deberían extender a dichos terceros.

[715] Cfr. Dictamen del Supervisor Europeo de Protección de Datos sobre el paquete legislativo relativo a las víctimas de la delincuencia, incluida la propuesta de Directiva por la que se establecen normas mínimas sobre los derechos, el apoyo y la protección de las víctimas de delitos y la propuesta de Reglamento relativo al reconocimiento mutuo de medidas de protección en materia civil, Publicado en el DOUE n° C 35/10, de 9.2.2012, p. 15.
[716] Dictamen 01/2013, de 26.02.2013, del Grupo de Trabajo del Artículo 29, p. 3.

1.1.3. Terceros sin relación con una infracción penal

La situación más delicada en relación los interesados cuyos datos son tratados en el ámbito de la prevención y represión penal, es la de las personas que no tienen ningún vínculo con el hecho delictivo investigado (artículo 5.e). En dichos casos, los grados de exigencia para autorizar el tratamiento de datos personales deben ser mayores, ya que la legitimidad para dicho tratamiento disminuye en la medida que el interesado no ha tenido participación alguna en los hechos. En tales casos, el tratamiento sólo debe permitirse bajo ciertas condiciones específicas, esto es, cuando sea absolutamente necesario para un propósito legítimo, bien definido y específico. Cabe recordar que el tratamiento sólo puede ser lícito en la medida que el fin sea la prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales; proteger los intereses vitales del interesado o de otra persona; o bien para la prevención de una amenaza inminente y grave para la seguridad pública.[717] No obstante, y aún estando en presencia de alguno de estos supuestos habilitantes, el tratamiento de datos personales de personas no sospechosas se debería limitar a un período acotado de tiempo y se debe prohibir el uso posterior de estos datos para otros fines distintos del que motivó su recolección. En esta misma línea, el GT29 ha señalado que sólo se puede procesar o tratar los datos de personas no sospechosas cuando sea indispensable para un propósito legítimo, bien definido y específico, limitado a evaluar la pertinencia de una de las categorías indicadas en el artículo 7 párrafo 1 (a) - (d), restringiendo su uso a un período de tiempo limitado y prohibiendo su posterior utilización.[718]

La evolución de las técnicas y métodos de aplicación de la ley en el ámbito de la prevención y represión penal en la última década, demuestran con claridad que todas estas categorías, que caen bajo la amplia denominación de «personas no sospechosas», necesitan una protección específica. Esta protección reforzada cobra especial importancia cuando el procesamiento de datos no se realiza en el contexto de una investigación o persecución penal, y sirve para poner freno al apetito de las autoridades encargadas de la persecución penal por obtener datos, ayudando a distinguir entre la información que «necesitan saber» para el cumplimiento de sus funciones de la

[717] Artículo 7 de la propuesta de Directiva.
[718] Dictamen 01/2013, de 26.02.2013, del Grupo de Trabajo del Artículo 29, p. 3 y 4.

información que sería «bueno tener».[719] En esta línea, el Grupo de Trabajo del artículo 29 entiende que el tratamiento de los datos de personas «no sospechosas» podría ser necesario en situaciones específicas, pero proponen normas particularmente estrictas para aquellas situaciones en las que el tratamiento no sirve a los efectos de una investigación o enjuiciamiento específico.[720]

Con el fin de proteger los datos de las personas no sospechosas, el Grupo de Trabajo del Artículo 29, ha sugerido la introducción de un nuevo artículo 7 bis, además del artículo 5, en la propuesta de Directiva de 2012. Este nuevo artículo 7 bis, tendría por finalidad asegurar que la diferenciación entre las diferentes categorías de interesados no sea sólo una carga administrativa, es decir, un requisito formal para habilitar el tratamiento, ya que la propuesta actual podría interpretarse en ese sentido. Para ello proponen que los Estados Miembros sólo puedan tratar los datos de personas no sospechosas si se cumplen los requisitos específicos señalados en el artículo propuesto y, por el contrario, que no se requiera la protección adicional cuando se procesan los datos de personas sospechosas. La elección del artículo 7 en vez del artículo 5, se debe a que en el primero se regula la legalidad del tratamiento.[721]

[719] Ídem.
[720] Ídem.
[721] La propuesta de enmienda del GT29 para un nuevo artículo 7 bis, relativa a los *Diferentes categorías de interesados*, es la siguiente: «1. Los Estados Miembros dispondrán que las autoridades competentes, a los efectos previstos en el artículo 1.1, sólo podrán tratar los datos personales de las siguientes distintas categorías de interesados: (a) las personas respecto de las cuales haya motivos razonables para creer que se han comprometido o están a punto de cometer un delito; (b) las personas condenadas por un delito; (c) las víctimas de un delito, o personas con respecto a las cuales existan razones para creer que podrían ser víctima de un delito; (d) Los terceros en el delito, como las personas que sean consideradas a testigos en investigaciones relacionadas con delitos penales o posterior procedimiento, o una persona que pueda proporcionar información sobre delitos , o un contacto o asociarse a una de las personas mencionadas en (a) y (b); *2. Los datos personales de otros interesados distintos de los mencionados en el apartado 1 sólo podrán ser tratados (a) el tiempo necesario para la investigación o el enjuiciamiento de un delito específico con el fin de evaluar la pertinencia de los datos para una de las categorías indicadas en el apartado 1, o (b) cuando dicho tratamiento es indispensable para propósitos específicos, preventivos o para los fines de análisis criminal, si y siempre que ello es legítimo, bien definido y específico y el tratamiento se limita única y exclusivamente para evaluar la pertinencia de los datos para una de las categorías indicadas en el apartado 1. Esto está sujeto a revisiones periódicas, que se realizará al menos cada seis meses. Se prohíbe cualquier otro uso.* 3. Los Estados Miembros dispondrán que las limitaciones y garantías adicionales, de acuerdo con la legislación nacional, se aplican al tratamiento posterior de los datos personales de los titulares de los datos mencionados en el párrafo 1 (c) y (d). [la traducción y el destacado es nuestro]. Cfr. Opinion 01/2013, *providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive*, WP 201, Adopted on 26 February 2013, p. 4.

1.1.4. Menores vinculados a infracciones penales

Un punto particularmente sensible es el tratamiento de datos personales de menores de edad, o de acuerdo a la nomenclatura de los acuerdos internacionales vigentes, de niños, niñas y adolescentes. En particular nos referimos al caso en que un menor sea considerado dentro de una investigación penal como autor, cómplice, encubridor o sospechoso de cometer un delito; o por otra parte, que sea víctima, testigo u otro tercero sin participación en el mismo. Pensemos, por ejemplo, en los casos de abusos sexuales, la explotación sexual y la pornografía infantil. En tales casos, cuando el interesado es menor de edad, ¿se consagra algún tipo de protección reforzada en la actual normativa europea de tratamiento de datos personales en el ámbito de la prevención y represión penal?

De conformidad con los criterios de los instrumentos internacionales más importantes[722], un niño es una persona natural con menos de 18 años de edad. Un niño es un ser humano en el sentido íntegro de la palabra, por tanto, debe gozar de todos los derechos de una persona, incluyendo el derecho a la protección de sus datos personales. No obstante, los niños se encuentran en una situación especial que debe considerarse desde dos perspectivas: la estática y la dinámica. Desde el punto de vista estático, el niño es una persona que aún no ha alcanzado la madurez física y psicológica; y desde el punto de vista dinámico, el niño se encuentra en el proceso de desarrollarse física y mentalmente para convertirse en adulto. En consecuencia, los Derechos del niño y su

[722] Entre los instrumentos internacionales aplicables, encontramos aquellos que se refieren a los derechos humanos en *general*, pero que contienen normas específicas sobre niños, tales como la Declaración Universal de Derechos Humanos, de 10.12.1948 (artículos 25, 26, n° 3); la Convención Europea para la Protección de los Derechos Humanos y Libertades Fundamentales, de 04.11.1950 (artículo 8); la Declaración de Helsinki, de junio de 1964 (Pr. I-11); el Pacto Internacional de Derechos Económicos, Sociales y Culturales, de 16.12.66 (artículo 10, n° 3); el Pacto Internacional de Derechos Civiles y Políticos, de 16.12.66 (Artículos 16 y 24) y el Protocolo opcional de 1de la misma fecha; y la Carta de los Derechos Fundamentales de la UE, de 07.12.2000 (Artículo 241); Por su parte, entre los instrumentos internacionales que se refiere *específicamente* a los derechos del niño, encontramos: la Declaración de Ginebra sobre los derechos del niño, 1923; la Convención de las Naciones Unidas sobre los derechos del niño, de 20.11.89; el Convenio nº 160 del Consejo de Europa, de 25.01.1932, sobre el ejercicio de los derechos de los niños; Declaración de las Naciones Unidas sobre los derechos del niño, 20/11/59; Recomendaciones de la Asamblea parlamentaria del Consejo de Europa sobre los distintos aspectos de la protección de los niños (n. 1071, 1074, 1121, 1286, 1551); Recomendaciones del Comité de Ministros del Consejo de Europa sobre la participación de los niños en la vida familiar R (98)8, y sobre la protección de los datos médicos, R (97), 5.; Convenio sobre las relaciones personales relacionadas con los menores, Consejo de Europa, n.192, de 15.05.2003.

ejercicio (incluyendo el de la protección de datos) deben expresarse de manera que se reconozcan ambas perspectivas.[723]

La forma jurídica que da cuenta de esta especial protección de los menores se denomina «principio de interés superior del menor».[724] Este principio lleva implícito el reconocimiento de dos cuestiones. En primer lugar, que la inmadurez del niño le hace vulnerable y ello debe compensarse mediante una protección y cuidados adecuados y, en segundo lugar, que el derecho del niño al libre desarrollo de su persona sólo puede disfrutarse adecuadamente con la asistencia o protección de otras entidades y/o personas.[725] Por tanto, quienes deben hacerse cargo de dicha protección son la familia, la sociedad y el Estado.

Cabe preguntarse entonces si la normativa europea sobre protección de datos personales contempla en sus disposiciones el reconocimiento del principio del interés superior del menor.

La Directiva 95/46/CE no hace ninguna referencia específica al tratamiento de datos personales de los menores de edad. No obstante, ésta se aplica a toda persona física, lo que indudablemente incluye a los menores de edad. Ahora bien, esta situación podría cambiar de aprobarse el Reglamento General de Protección de Datos en los términos actuales, ya que éste dedica el artículo 8 a regular las condiciones para la

[723] Al respecto, véase Documento de trabajo 1/08 sobre la protección de datos personales de los niños (Directrices generales y el caso especial de los colegios), del Grupo de Trabajo del Artículo 29, WP 147, de 18.2.2008, p. 2 y ss. El GT29, ya se había pronunciado en otros dictámenes anteriores sobre el tratamiento de datos de menores: Dictamen 3/2003 sobre el código de conducta de la FEDMA; Dictamen5/2005, sobre la geolocalización; y Dictamen 3/2007, sobre Visados y Biometría, todos los cuales incluyen determinados principios o recomendaciones en relación con la protección de datos de los niños.

[724] Este principio se encuentra reconocido en el la Convención de las Naciones Unidas sobre los derechos del niño (Artículo 3) y, posteriormente, ha sido reafirmado por el Convenio n° 192 del Consejo de Europa (Artículo 6) y la Carta de derechos fundamentales de la Unión Europea (Artículo 24, N. 2). El principio del interés superior del menor, se basa en que una persona que aún no ha alcanzado la madurez física y psicológica necesita más protección que otros, por tanto, su objetivo es mejorar las condiciones de los niños y pretende reforzar el derecho de los niños al desarrollo de su personalidad. Ello trae como consecuencia, que todas las entidades, públicas o privadas, así como los progenitores y a otros representantes de los niños que tomen decisiones relativas a los mismos deben respetar este principio. Al respecto véase Isaac RAVETLLAT BALLESTÉ, "El interés superior del niño: concepto y delimitación del término", *Educatio siglo XXI: Revista de la Facultad de Educación* N° 30 (2012): pp. 89–108.

[725] El «derecho a la protección» se incluyó en la Declaración Universal de Derechos Humanos (Artículo 25), y se confirmó en el Pacto Internacional de Derechos Civiles y Políticos (Artículo 24), en el Pacto Internacional de Derechos Económicos, Sociales y Culturales (Artículo 10, N. 3), y, más recientemente, en la Carta de Derechos Fundamentales de la Unión Europea (Artículo 24).

licitud del tratamiento de los datos personales de los niños en relación con los servicios de la sociedad de la información que se les ofrecen directamente.[726] Además, en diversos considerandos de la propuesta de Reglamento, se hace referencia a la necesidad de protección específica de los datos personales de los niños.[727] Lo anterior, da cuenta de la importancia que ha adquirido este tema en los últimos años.[728]

Por su parte, en lo referido a la normativa de protección de datos personales en el ámbito de la prevención y represión penal, la Decisión Marco 2008/977/JAI, actualmente vigente, no contempla ninguna disposición ni referencia en sus considerandos al tratamiento de datos personales de los menores de edad. En el proyecto de Directiva que deroga y reemplaza la citada Decisión Marco, la regulación es mucho más tímida que la propuesta de Reglamento general. Si bien, ambas propuestas

[726] Otras disposiciones de la propuesta de nuevo Reglamento, también hacen mención expresa a los menores de edad, v.g. el artículo 11 (derechos del interesado/transparencia y modalidades); artículo 33.d (evaluación de impacto relativa a protección de datos y evaluación previa); art. 38 (códigos de conducta); art. 52.2, funciones de la autoridad de control.

[727] Así por ejemplo, el considerando 29, señala que «Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos en relación con el tratamiento de datos personales. Con el fin de determinar cuándo se considera que una persona es un niño, el presente Reglamento debe asumir la definición establecida en la Convención de las Naciones Unidas sobre los derechos del niño». Por su parte, el considerando 38, establece que «El interés legítimo de un responsable puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado. Ello necesitaría una evaluación meticulosa, especialmente si el interesado fuera un niño, pues los niños merecen una protección específica…». El considerando 46, que se refiere al principio de transparencia, establece que «…Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte específicamente debe facilitarse en un lenguaje claro y llano que puedan comprender con facilidad». Por último, el considerando 53, al referirse al «derecho al olvido», establece que «…Este derecho es particularmente pertinente si los interesados hubieran dado su consentimiento siendo niños, cuando no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quisieran suprimir tales datos personales especialmente en Internet…».

[728] Para un estudio detallado del tema, en sus diversas manifestaciones, véase Agencia de Protección de Datos de la Comunidad de Madrid, «Solicitud de información de menores a centros escolares por parte de una Policía Local», *N° 13* (2005); Agencia de Protección de Datos de la Comunidad de Madrid, «La Privacidad de los menores: reto del Siglo XXI para todos los poderes públicos», *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid* N° 60 (2012); Francisco Javier DURÁN RUIZ, «La necesaria intervención de las administraciones públicas para la preservación del derecho fundamental a la protección de datos de los menores de edad», en *I Congreso sobre retos sociales y jurídicos para los menores y jóvenes del siglo XXI*, ed. Francisco Javier DURÁN RUIZ (Comares, 2013); Antoni FARRIOLS i SOLÁ, «Los menores y adolescentes ante el uso de las tecnologías de la información y la protección de los datos de carácter personal», *Base Informática* N° 44 (2009): pp. 41-46; Isidro GÓMEZ-JUÁREZ SIDERA, «Reflexiones sobre el derecho a la protección de datos de los menores de edad y la necesidad de su regulación específica en la legislación española», *Revista Aranzadi de derecho y nuevas tecnologías* N° 11 (2006): pp. 71-88; Antonio Enrique PÉREZ LUÑO, «La protección de los datos personales del menor en Internet», *Anuario de la Facultad de Derecho (Universidad de Alcalá)* N° 2 (2009): pp. 143-175; Antonio Enrique PÉREZ LUÑO, «El consentimiento de los menores: Título II. Principios de la Protección de Datos. artículo 6», en *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, ed. Antonio TRONCOSO REIGADA (Madrid: Civitas, 2010), pp. 473-494.

(Reglamento y Directiva) adoptan la definición de «niño», basado en la Convención de las Naciones Unidas sobre los Derechos del Niño,[729] la propuesta de Directiva no dedica un artículo en particular para regular el tratamiento de datos personales de los menores de edad, y sólo hace referencia expresa a los niños a propósito de las funciones que debe desempeñar las autoridades de control, imponiendo a las mismas una «especial atención» en caso de tratamiento de datos personales de niños en el ámbito de la prevención y represión penal.[730] Por tanto, podemos concluir que de participar un menor en un hecho delictivo, sea como sujeto activo, pasivo o tercero, el actual y futuro marco normativo de la Unión Europea sobre protección de datos personales en el ámbito de la prevención y represión penal, no les brinda ninguna especial protección, aplicándose las reglas generales a su respecto. La única situación de excepción estaría dada por los delitos de connotación sexual en contra de menores, donde la propuesta de Directiva para el ámbito de la prevención y represión penal hace un reenvío a la Directiva 2011/92/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011.[731]

1.2. Personas jurídicas (morales)

En principio, tanto las personas físicas como las jurídicas podrían ser titulares del derecho a la protección de datos. De hecho, varios países de la Unión incluyen la protección de las personas jurídicas dentro del ámbito de aplicación de su normativa nacional sobre protección de datos.[732] En lo que respecta a la normativa europea sobre protección de datos, el Convenio 108 del Consejo de Europa, establece como criterio

[729] Mencionado también en el artículo 2, letra a), de la Directiva 2011/92/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo. Publicada en el DOUE n° L 335, 17.12.2011, p. 1.

[730] «Artículo 45. Funciones.1. Los Estados Miembros dispondrán que la autoridad de control: 2. Cada autoridad de control promoverá la sensibilización del público sobre los riesgos, normas, garantías y derechos relativos al tratamiento de datos personales. *Las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención*» [el destacado es nuestro]. Cfr. Propuesta de Directiva de 2012, p. 50 y 51.

[731] Cfr. considerando 74 de la propuesta de Directiva de 2012.

[732] Entre los países que extiende el ámbito de aplicación de su normativa sobre protección de datos a las personas jurídicas, v.g.: Austria, Dinamarca, Italia y Luxemburgo. Por el contrario, entre los países que excluyen expresamente a las personas jurídicas del ámbito de aplicación de las normas nacional sobre protección de datos, encontramos a Alemania, Bélgica, España, Finlandia, Francia, Grecia, Holanda, Irlanda, Portugal, Suecia y Reino Unido. En España se ha dado una interesante discusión en la doctrina respecto de si las personas jurídicas pueden o no ser titulares del derecho a la protección de datos. Por todos, véase María del Carmen GUERRERO PICÓ, *El Impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, pp. 222–224; María Mercedes SERRANO PÉREZ, *El derecho fundamental a la protección de datos. Derecho español y comparado*, pp. 256–267.

general, en su artículo 1, que sólo las personas físicas pueden ser titulares del derecho a la protección de datos, sin perjuicio de dejar al arbitrio de los Estados la posibilidad de ampliar su aplicación a las personas jurídicas.[733] Por su parte, y sin desconocer que ha sido un tema discutido por la doctrina, la Directiva 95/46/CE (artículo 1.1.), también se decanta por las personas físicas como únicos sujetos activos de este derecho.[734] Ahora bien, en el ámbito específico de la protección de datos con fines de prevención o represión penal, tanto la Decisión Marco 2008/977/JAI como la propuesta de Directiva de 2012, que pretende reemplazarla, restringen su ámbito de aplicación sólo a las personas físicas (naturales).[735]

2. LOS DERECHOS DE LOS TITULARES

El derecho fundamental a la protección de datos personales reconoce a los titulares de los datos un conjunto de facultades para hacer efectiva la autodeterminación informativa. Tradicionalmente dichas facultades, que permiten al interesado controlar el uso y destino de los datos personales, han sido los derechos de acceso, rectificación y cancelación.[736] A estos derechos, y producto de los avances que han experimentado los instrumentos normativos que los regulan, se han ido agregando, concretando y

[733] Cfr. artículo 3.2.b) del Convenio 108 del Consejo de Europa, de 1981.
[734] Ello se deduce del tenor literal del considerando 24 de la Directiva 95/47/CE. En contra, véase Mónica ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa* (Valencia: Tirant lo Blanch, 2006), p. 302.
[735] Cfr. artículo 2 a) de la Decisión Marco; artículo 3 a) de la propuesta de Directiva de 2012. Respecto de ésta última, la única referencia que podría dar lugar a una interpretación amplia del sujeto activo del derecho a la protección de datos, con la finalidad de incluir a las personas jurídicas como sujetos de los mismo, sería el considerando 62, que dispone que «Toda persona física o jurídica debe tener derecho a presentar un recurso judicial contra las decisiones de una autoridad de control que le conciernan…». No obstante, en el articulado de la propuesta dicha postura no encuentra sustento, ya que ésta sólo hace referencia a las personas físicas como titular del derecho a la protección de datos. Cfr. COM(2012) 10 final, p. 24.
[736] Dentro del proceso de configuración y concretización de los derechos que integran la protección de datos personales, la labor del TEDH ha sido fundamental. Dicho Tribunal, ya en el año 1978, partiendo del artículo 8 del CEDH y apoyado también en los primeros instrumentos internacionales sobre la materia, dictó un fallo donde estableció las facultades que integran el derecho a la protección de datos, entre los que se encuentran, el derecho de información, acceso, rectificación y a la libre disposición de los datos. Cfr. STEDH de 6.9.1978, caso *Klass*. Al respecto véase ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, 97, y la bibliografía citada por la autora; y SERRANO PÉREZ, *El derecho fundamental a la protección de datos. Derecho español y comparado*, 343

especificando otros derechos, tales como, los de información, oposición, a presentar un recurso y a ser indemnizado.[737]

En el presente apartado nos proponemos realizar una revisión de la evolución y situación actual de los derechos a la protección de los datos personales consagrados particularmente para el caso de la prevención y represión penal, sin perjuicio de referirnos a las reglas generales cuando el caso lo amerite.

La primera regulación internacional específica dictada en Europa sobre la materia, es el Convenio 108 del Consejo de Europa de 1981, el cual trató esta materia bajo la denominación genérica de «garantías complementarias para la persona concernida».[738] En ella, se reconoce a los titulares de los datos un conjunto de derechos que pueden ejercer para controlar el tratamiento de los mismos por parte de terceros, sean estas personas naturales o jurídicas, públicas o privadas.[739] Por su parte, la Directiva 95/46/CE también reconoce a los titulares de los datos el derecho a la información, acceso, oposición, rectificación y cancelación.[740]

Llama la atención que la CDFUE, al reconocer el derecho fundamental a la protección de datos personales como un derecho fundamental y autónomo en el artículo 8, sólo haga referencia expresa a los derechos de «acceso» y «rectificación».[741] Ahora bien, si tomamos en cuenta que para la elaboración de dicho artículo se tomaron en consideración tanto el artículo 286 del TCE (sustituido por el artículo 16 del Tratado de Funcionamiento de la Unión Europea y el artículo 39 del Tratado de la Unión Europea) y la Directiva 95/46/CE, como el artículo 8 del CEDH y el Convenio 108 del Consejo de Europa, según se señala expresamente en la memoria explicativa de la CDFUE, entendemos que el conjunto de derechos reconocidos por dichos instrumentos son plenamente válidos para determinar el conjunto de facultades que confiere este derecho

[737] Sobre los derechos véase Olga ESTADELLA YUSTE, *La protección de la intimidad frente a la transmisión internacional de datos personales* (Madrid: Tecnos, 1995), 67-68; Álvaro SÁNCHEZ BRAVO, *La protección del derecho a la libertad informática en la Unión Europea* (Sevilla: Universidad de Sevilla, 1998), 79; ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, 163–165. Respecto de los derechos que se reconoce en el sistema jurídico español de protección, véase GUERRERO PICÓ, *El Impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, 289–311.
[738] Artículo 8 del Convenio 108 de 1981.
[739] Artículo 5 del Convenio 108.
[740] Artículos 10, 11, 12 y 14 de la Directiva 95/46/CE.
[741] Artículo 8.2. del TFUE.

al titular del mismo.[742] De esta forma se supera cualquier interpretación en el sentido de establecer una prioridad o exclusión de algunas de las facultades inherentes al ejercicio del derecho a la protección de datos.

Cabe recordar que antes de Decisión Marco 2008/977/JAI, ante la ausencia de una norma de carácter general que regulara el tratamiento de datos personales en el ámbito de la cooperación policial y judicial, se dictaron diversas disposiciones particulares en cada uno de los cuerpos normativos de la Unión Europea, donde se necesitaba regular dichas materias. Así, por ejemplo, la Decisión 2008/615/JAI, que incorpora al ordenamiento comunitario las principales disposiciones sobre el Tratado de Prüm, reenvía a las disposiciones de los Estados Miembros la regulación sobre el reconocimiento, ejercicio y limitaciones de los derechos de las personales en relación al tratamiento de sus datos personales.[743] Lo mismo ha ocurrido con los grandes sistemas de información que se manejan en el antiguo tercer pilar comunitario (v.g. SIS y SIV), cuyas normas reguladoras reconocen los derechos de acceso, así como los de rectificación y cancelación.[744] Por su parte, los Reglamentos de Europol y Eurojust, también reconocen a los titulares de los datos algunos derechos, pero de una forma más limitada.[745] En cualquier caso, con algunas excepciones puntuales, hay que reconocer que en todos los ámbitos del derecho comunitario se está realizando un esfuerzo por

[742] El artículo 8 del CDFUE, se basa en el artículo 286 del Tratado constitutivo de la Comunidad Europea y en la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31), así como en el artículo 8 del CEDH y en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, ratificado por todos los Estados Miembros. El artículo 286 del Tratado CE ha sido sustituido por el artículo 16 del Tratado de Funcionamiento de la Unión Europea y el artículo 39 del Tratado de la Unión Europea. Conviene señalar asimismo el Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1). La Directiva y el Reglamento mencionados establecen condiciones y límites para el ejercicio del derecho a la protección de los datos de carácter personal. Cfr. Explicación relativa al artículo 8 —Protección de datos de carácter personal— [actualizada y corregida] de la Carta Europea de Derecho Fundamentales, publicada en el DOUE n° C 303, de 14.12.2007, p. 20.

[743] Sobre el Tratado de Prüm y la Decisión 2008/615/JAI, véase *supra* apartado 3 del capítulo sexto de este trabajo.

[744] Artículo 109 a 111 del Convenio Schengen; artículo 15 Convenio SIA..

[745] Cfr. Decisión Europol 2009/371/JAI (artículos 30 a 33). Cabe señalar que en la propuesta de Reglamento General de Europol COM (2013) 173 final, en el Capítulo VII, titulado «Garantías en materia de protección de datos», se regula con más detalle los derecho de acceso, rectificación, cancelación y bloqueo (artículos 34 a 40). Por su parte, el Reglamento interno de Eurojust relativo al tratamiento y protección de datos personales, (2005/C 68/01), reconoce también los derechos de información, acceso, rectificación, cancelación, bloqueo y eliminación (artículos 9, 19 a 22). Al respecto, véase también el artículo 18 del Reglamento Eurodac; y los artículos 11 y 17 del Reglamento Eurostat, que sólo reconoce el derecho de acceso a las estadísticas comunitarias.

reconocer los mismos derechos para los titulares de los datos, con el fin de conseguir una eficaz protección de las personas respecto al tratamiento de sus datos personales.

2.1. Derecho a la información

La primera facultad que otorga el derecho a la protección de datos, es el derecho a la información o a ser informado, es decir, que se le comunique al interesado qué información personal ha sido recogida, registrada y con qué finalidad va a ser utilizada. Este derecho tiene como contrapartida la obligación de la persona o institución responsable del tratamiento, de contar con políticas transparentes en lo que al tratamiento de datos de carácter personal se refiere.[746] La importancia del derecho a la información, radica en que generalmente constituye una condición indispensable para el ejercicio de las otras facultades que emanan del derecho a la protección de datos personales.[747]

En cuanto al reconocimiento del derecho a la información en los diversos textos jurídicos vigentes en la Unión Europea, la situación es disímil.[748] Tanto el Convenio 108 del Consejo de Europa[749], como la Carta de Derechos Fundamentales de la Unión Europea, no reconocen explícitamente el derecho a la información del titular de los datos, sino más bien se limitan a consagrar el derecho de acceso. No obstante, dicho

[746] Esta obligación se denomina «principio de transparencia», y está recogida en el artículo 11 de la Resolución de Madrid, relativa a estándares internacionales sobre protección de datos personales y privacidad, adoptada por la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad de 5.11.2009.

[747] No debe confundirse el derecho a la información como una facultad inherente a la protección de datos con el derecho a recibir y entregar la información. Como lo ha señalado el TEDH, el fundamento de este derecho de acceso, forma parte del derecho a la protección de datos garantizado por el artículo 8 del CEDH y no en el derecho a recibir información reconocido en el artículo 10 del CEDH; «mientras que el artículo 10 del CEDH se refiere a información que otros desean obtener, el artículo 8 del CEDH hace referencia a información confidencial que el titular no desea develar». Además, el TEDH ha repetido en numerosas ocasiones que «del artículo 10 CEDH no se puede deducir un derecho general de acceso a la información», mientras que sí ha reconocido que «el contenido del artículo 8 del CEDH puede ampliarse hasta incluir el derecho a buscar información sobre la vida privada en determinadas situaciones». Cfr. STEDH de 26 de marzo de 1987, caso *Leander* y STEDH de 7 de julio de 1989, caso *Gaskin*. Al respecto véase ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, 105.

[748] En los Estados de la Unión Europea, este derecho ha sido recogido de diversas maneras en cuento a la forma de entregar la información, así como respecto del momento y el contenido de la misma. Al respecto véase Ibid., 494-495

[749] Artículo 8 del Convenio 108, titulado *Garantías complementarias para la persona concernida*, reconoce en su letra a) que cualquier persona deberá poder «Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero».

derecho debe ser reconocido al titular de los datos precisamente para que pueda disponer de ellos libremente, y decidir si quiere o no que los mismos sean tratados.[750] En lo que respecta a la Directiva 95/46/CE, en ella se hace referencia a este derecho como una obligación del responsable del tratamiento, es decir, no se reconoce como un derecho del interesado, sino sólo como la obligación de informar por parte del responsable del tratamiento de los datos personales, distinguiendo si los datos han sido o no recogidos directamente del interesado.[751]

En el ámbito específico del tratamiento de datos personales por parte de la policía o los tribunales con fines de prevención o represión penal, encontramos, en primer lugar, la Recomendación (87) 15, la cual consagra el derecho a la información y, como contrapartida, la obligación de los órganos encargados de la prevención y represión penal de informar al titular de los datos sobre un futuro o actual tratamiento de sus datos personales.[752] La normativa actualmente vigente, la Decisión Marco 2008/977/JAI, destina el artículo 16 a regular el derecho a la información por parte del interesado. En ella, se impone la obligación a los Estados de informar al titular de los datos respecto del tratamiento que se esté llevando a cabo por las autoridades competentes. No obstante, el ejercicio del derecho queda supeditado a lo dispuesto en la legislación de cada Estado de la Unión, lo que obviamente genera o puede generar disparidad de criterios en cuanto al reconocimiento del derecho y la operatividad del mismo.[753]

Esta situación podría cambiar, si se aprueba la propuesta de Directiva que reemplaza y deroga la Decisión Marco antes citada, ya que aquella contempla un

[750] Así la ha entendido también el TJCE. Cfr. STJCE de 14 de septiembre de 2000, caso *The Queen and the Ministry cf Agriculture, Fischeries and Food*, y Conclusiones del Abogado General Alber presentadas el 10.2.2000. Al respecto véase MAR, p. 259-261.

[751] Artículos 10 y 11 de la Directiva 95/46/CE. Esta omisión es considerada por algunos autores como inaceptable, al respecto véase SÁNCHEZ BRAVO, *La protección del derecho a la libertad informática en la Unión Europea*, 139. ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, 304.

[752] El Principio 6 de la Recomendación (87) 15, titulado *La publicidad, derecho de acceso a los archivos de la policía, el derecho de rectificación y derecho de los recurso de casación*, reconoce en el numeral 6.1: «La autoridad de supervisión debe tomar medidas a fin de cerciorarse de que el público es informado de la existencia de expedientes que son objeto de notificación, así como de sus derechos en lo que respecta a estos archivos. La aplicación de este principio debe tener en cuenta la naturaleza específica de los archivos *ad hoc*, en particular, la necesidad de evitar un perjuicio grave a la ejecución de una obligación legal de los órganos de policía». [traducción del autor].

[753] Artículo 16.1. de la Decisión Marco 2008/977/JAI. *Información al interesado*. «1. Los Estados Miembros se harán cargo de que el interesado esté informado de lo relativo a la recopilación o tratamiento de datos personales por sus autoridades competentes, conforme al Derecho nacional».

artículo mucho más explícito y detallado que ésta. De partida, la propuesta junto con especificar la obligación de los Estados Miembros de garantizar la información al interesado, amplía y detalla el contenido de la información que se le debe facilitar al interesado.[754] En efecto, el artículo 11.1, tomando como base los artículos 10 y 11 de la Directiva 95/46/CE, dispone que: «1. Cuando se recojan datos personales relativos a un interesado, los Estados Miembros velarán por que el responsable del tratamiento tome todas las medidas oportunas para facilitar al interesado, al menos, la siguiente información: a) la identidad y los datos de contacto del responsable del tratamiento y del delegado de protección de datos; b) los fines del tratamiento a que se destinan los datos personales; c) el plazo durante el cual se conservarán los datos personales; d) la existencia del derecho a solicitar del responsable del tratamiento el acceso a los datos personales relativos al interesado y su rectificación, su supresión o la limitación de su tratamiento; e) el derecho a presentar una reclamación ante la autoridad de control contemplada en el artículo 39 y los datos de contacto de la misma; f) los destinatarios o las categorías de destinatarios de los datos personales, en particular en terceros países u organizaciones internacionales; g) cualquier otra información en la medida en que resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado, habida cuenta de las circunstancias específicas en las que se traten los datos personales».

En relación al momento en el cual se debe informar al interesado que sus datos son o van a ser objeto de un tratamiento, la propuesta establece una distinción. En caso que los datos sean directamente recabados del interesado, se impone la obligación de informar en el momento en que los datos personales se obtengan de él interesado[755], en cambio, cuando los datos personales no se recojan del interesado, la norma establece que se debe informar al titular de los datos al momento del registro o en un plazo razonable después de la recogida, habida cuenta de las circunstancias específicas en que se traten los datos.[756] Éste último supuesto es el más controvertido, ya que generalmente en una investigación policial o judicial no se informa al titular de los datos que está siendo objeto del mismo al inicio de una investigación. Pensemos por ejemplo, en el caso que un tribunal haya autorizado llevar a cabo medidas de vigilancia secretas, tales

[754] Cfr. Propuesta de Directiva COM (2012) 10 final, de 25.1.2012, p.
[755] Artículo 11.3. a) de la Propuesta de Directiva.
[756] Artículo 11.3. b) de la Propuesta de Directiva.

como escuchas telefónicas, interceptación del correo electrónico, fotografiar o filmar a un sospechoso, entre otras. En tales casos, y con las garantías adecuadas para evitar abusos, se podría permitir que el interesado sea informado con posterioridad, al término de dichas medidas. Con ello se permite, por una parte, el éxito de una investigación, y por otra, que el interesado conozca que fue objeto de una medida de vigilancia con la finalidad de que pueda ejercer sus derechos, mediante los procedimientos que considere pertinentes.

Como se puede apreciar, en estos casos es necesario conciliar la defensa de la seguridad en una sociedad democrática con la salvaguarda de los derechos individuales, buscando un equilibrio entre la necesidad del secreto y el deber de informar a los titulares de los datos. El TEDH consciente de los peligros que puede conllevar la obtención de datos sin consentimiento de su titular, así como de los posibles usos posteriores que se les pueda dar a dicha información, exige que se den una serie de requisitos para poder afirmar la legalidad de la obtención de los datos, entre ellos, que se informe al afectado de los datos que, sin su conocimiento y aún declarados confidenciales, sean relevantes con relación a determinados aspectos de su personalidad. Así, en el caso *Klass*, el TEDH confirmó que para que una intervención de escuchas telefónica logre sus objetivos no puede ser conocida por quienes son objeto de ella, y fijó como exigencias para que dicha medida fuera compatible con las garantías del CEDH, además de un control judicial, que se informara a los interesados sobre las medidas de vigilancia una vez que hubieran concluido.[757] En la misma línea, el TEDH establece que cuando los datos puedan ser considerados secretos, por estar relacionados con la seguridad del Estado, deben existir las garantías suficientes para hacer compatibles la seguridad del Estado con la vida privada del titular de los datos.[758]

Otro tema importante vinculado al derecho a la información, es la posibilidad de establecer excepciones o limitaciones al mismo. Sin perjuicio que este tema será abordado de manera detallada en un apartado posterior[759], cabe señalar que la propuesta de Directiva regula de manera bastante generosa la posibilidad de establecer excepciones a la obligación de informar, ya que deja al criterio de los Estados

[757] STEDH de 6.9.1978, caso *Klass*.
[758] SSTEDH de 26.3.1987, caso *Leander*; y de 24.4.1990, caso *Huvig*.
[759] Al respecto véase *infra* apartado 3 de este capítulo.

Miembros determinar las categorías de tratamiento de datos que pueden acogerse, en su totalidad o en parte, a dichas exenciones.[760] Señala la propuesta que: «Los Estados Miembros podrán adoptar medidas legislativas por las que se retrase, limite o exima la puesta a disposición del interesado de la información en la medida y siempre que dicha limitación total o parcial constituya una medida necesaria y proporcional en una sociedad democrática, teniendo debidamente en cuenta los intereses legítimos de la persona en cuestión: a) para evitar que se obstaculicen pesquisas, investigaciones o procedimientos jurídicos o de carácter oficial; b) para evitar que se prejuzgue la prevención, detección, investigación y enjuiciamiento de infracciones penales o para la ejecución de sanciones penales; c) para proteger la seguridad pública; d) para proteger la seguridad nacional; e) para proteger los derechos y libertades de otras personas».[761] Estas excepciones tienen como referencia el artículo 13 de la Directiva 95/46/CE y el artículo 17 de la Decisión Marco 2008/977/JAI, y ponen énfasis en la exigencia básica ser «proporcionadas y necesarias en una sociedad democrática para el ejercicio de las tareas de las autoridades competentes».[762]

Por último, el artículo 10 de la propuesta de Directiva introduce la obligación de los Estados Miembros de ofrecer información de fácil acceso y comprensión, inspirada especialmente en el principio 10 de la Resolución de Madrid relativa a estándares internacionales sobre protección de datos personales y privacidad[763], y obliga a los responsables del tratamiento a establecer procedimientos y mecanismos para facilitar el ejercicio de los derechos del interesado. Ello incluye la obligación de que el ejercicio de los derechos sea, en principio, gratuito.[764]

[760] Artículo 11.5. de la propuesta de Directiva.
[761] Artículo 11.4 de la propuesta de Directiva.
[762] Cfr. Propuesta de Directiva COM (2012) 10 final, de 25.1.2012, p. 9.
[763] Resolución de Madrid, *relativa a estándares internacionales sobre protección de datos personales y privacidad*, adoptada por la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad de
5.11.2009.
[764] Al respecto, el considerando 28 de la propuesta de Directiva establece que «para poder ejercer sus derechos, cualquier información que se facilite al interesado debe ser fácilmente accesible y fácil de entender, utilizando un lenguaje sencillo y claro». Cfr. Propuesta de Directiva COM (2012) 10 final, de 25.1.2012, p. 8 y 19.

2.2. Derecho de acceso

El derecho de acceso es una de las facultades esenciales que integra la protección de datos personales. Permite a los interesados ejercer un **control** sobre los datos personales conservados por terceros, ya que en principio, cualquier persona que así lo solicite pueda consultar información que sobre él se haya introducido en un fichero o banco de datos, en la forma que determine la legislación pertinente.[765] De esta manera, reconocer el derecho de acceso permite que el ciudadano pueda acceder a los ficheros o archivos que contengan sus datos personales y saber cuáles de ellos han sido tratados. También hay que consignar que este derecho no sólo sirve para conocer información relativa a los datos concretos de carácter personal objeto de tratamiento, sino también sobre el origen de éstos, las finalidades de los correspondientes tratamientos y los destinatarios o las categorías de destinatarios a quienes se comuniquen o pretendan comunicar dichos datos.[766]

Antes de seguir con el análisis del derecho de acceso, hay que advertir sobre un punto. No se debe confundir el derecho de acceso a los datos personales por parte del titular de los mismos, en tanto ejercicio del derecho a la protección de datos personales, con el derecho de acceso a la información contenida en archivos, registros y documentos, ya sea de las Instituciones de la Unión, ya sea de los Estados por parte de un tercero, que genéricamente se le denomina también «derecho de acceso a los documentos» o «derecho a una buena administración».[767]

---

[765] Autoridades de Control Común de Schengen, *Guía para el ejercicio del derecho de acceso*, 13.10.2009. En este documento se describe el procedimiento para ejercer el derecho acceso en cada uno de los países del espacio Schengen.

[766] Resolución de Madrid, relativa a *estándares internacionales sobre protección de datos personales y privacidad*, adoptada por la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad de
5.11.2009, p. 19.

[767] Éste derecho se encuentra reconocido en el artículo 41 de la Carta de Derechos Fundamentales de la Unión Europea. "Sobre este derecho el TJCE se ha pronunciado en diversas ocasiones. Al respecto, véase STJCE de 6 de diciembre de 2001, caso *Hautala*, y las Conclusiones del Abogado General Léger presentadas el 10 de julio de 2001; STJCE de 22 de enero de 2004, caso *Mattila*; STJCE de 11 de enero de 2000, caso *Vander Wal*; y de 6 de marzo de 2003, caso *Interporc*. Véase asimismo, el Reglamento (CE nº 1049/2001, del Parlamento Europeo y del Consejo, de 30 de mayo, relativo al acceso del público a los documentos del Parlamento, del Consejo y de la Comisión. Estos derechos se reconocen, respectivamente, en los arts. 1-50, II-102 yII-101.2.bl del Tratado que establece la Constitución Europea.

El derecho de acceso a los datos personales se encuentra reconocido en diversos textos legales europeos. En el ámbito del Consejo de Europa, como hemos señalado anteriormente, la jurisprudencia del TEDH ha consagrado la protección de datos personales como una dimensión informacional del derecho a la vida privada reconocido en el artículo 8 del Convenio Europeo de Derechos Humanos.[768] En consecuencia, deberíamos considerar el derecho de acceso como una facultad inherente al derecho a la protección de datos y, por tanto, amparado por el Convenio. No obstante, debemos precisar que la interpretación del TEDH no ha sido explícita al respecto, ya que no deduce un derecho de acceso a la protección de datos garantizado por el artículo 8 del CEDH, sino que deja abierta dicha posibilidad. En efecto, el TEDH no lo reconoce de una forma general, sino en cada caso concreto.[769] Por su parte, el Convenio 108 reconoce expresamente al titular de los datos la facultad de conocer la existencia de un fichero, su finalidad, así como la identidad del responsable del mismo.[770]

Por otro lado, en el ámbito de la Unión Europea, este derecho, junto con el de rectificación, son los únicos derechos que se mencionan expresamente en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea.[771] En lo que respecta a la Directiva 95/46/CE, este derecho también tiene un reconocimiento expreso en su artículo 12, el cual obliga a los Estados Miembros a garantizar a todos los interesados el derecho de obtener del responsable del tratamiento: «a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos: la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos; la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos; el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos

[768] Respecto del reconocimiento del derecho a la protección de datos como parte integrante del derecho a la vida privada en el CEDH, véase *supra* apartado 1 del capítulo cuarto de este trabajo.
[769] Cfr. STEDH de 7 de julio de 1989, caso *Gaskin*, en la que el TEDH sostuvo que no estaba llamado a decidir en abstracto sobre cuestiones generales de principios en ese terreno, sino a solventar el caso concreto. Al respecto, véase Mónica ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, p. 105 y la bibliografía citada por la autora.
[770] Artículo 8, letra a) del Convenio 108 de 1981.
[771] Artículo 8.2. de la CDFUE.

referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15».[772]

Ahora bien, en lo que se refiere al tema específico de esta tesis, el primer texto que reguló el derecho de acceso en la protección de datos personales, fue la Recomendación (87) 15 del Consejo de Europa.[773] En la aún vigente Decisión Marco 2008/977/JAI se regula el derecho de acceso en un artículo específico.[774] El primer apartado se destina a especificar qué tipo de información puede solicitar el interesado, en los siguientes términos: «1. Todo interesado que lo solicite con una periodicidad razonable tendrá derecho a obtener, sin restricciones y sin retrasos ni gastos excesivos: a) al menos la confirmación, por parte del responsable del tratamiento o de la autoridad nacional de control, de que se han transmitido o puesto a disposición datos que le conciernen, e información sobre los destinatarios o categorías de destinatarios a los que se han remitido los datos y la comunicación de los datos que se están tratando, o b) al menos la confirmación de la autoridad nacional de control de que se han realizado todas las comprobaciones necesarias».[775] En los siguientes apartados el artículo 17 de la Decisión Marco establece la posibilidad de que los Estados Miembros puedan adoptar medidas legislativas para limitar o denegar el acceso a la información al titular de los datos.

En el caso que el Estado miembro quiera establecer una medida que limite el derecho de acceso, la Decisión Marco exige que junto tomar en cuenta los intereses legítimos del interesado, la medida sea necesaria y proporcionada: «a) para evitar que se obstaculicen investigaciones o procedimientos jurídicos o de carácter oficial; b) para evitar que se obstaculice la prevención, detección, investigación y enjuiciamiento de infracciones penales o la ejecución de sanciones penales; c) para proteger la seguridad pública; d) para proteger la seguridad del Estado; e) para proteger al interesado o los derechos y libertades de terceros».[776]

---

[772] Cfr. Considerando 41 de la Directiva 95/46/CE.
[773] Principio 6. *La publicidad, derecho de acceso a los archivos de la policía, el derecho de rectificación y derecho de los recursos de casación*. «6.2. El interesado debe ser capaz de obtener acceso a un archivo de la policía en intervalos de periodos razonable y sin excesiva demora, de conformidad con las disposiciones previstas por la legislación nacional» [traducción del autor].
[774] Artículo 17 de la Decisión Marco 2008/977/JAI.
[775] Artículo 17.1 de la Decisión Marco 2008/977/JAI.
[776] Artículo 17.2 de la Decisión Marco 2008/977/JAI.

La Decisión Marco establece la obligación de comunicar por escrito al interesado los motivos materiales o jurídicos que se tuvieron en cuenta para la denegación o limitación del derecho de acceso al interesado. No obstante, esta comunicación puede omitirse cuando exista algún motivo de los indicados en el apartado 2, letras a) a e). En todos estos casos se debe poner en conocimiento del interesado los medios de impugnación de dicha decisión, es decir, que puede recurrir ante la autoridad nacional de control o a los juzgados o tribunales competentes.[777]

En lo que respecta a la propuesta de Directiva que reemplaza y deroga la Decisión Marco 2008/977/JAI de 25 de enero de 2012, el artículo 12 establece la obligación de los Estados Miembros de garantizar el derecho del interesado a acceder a sus datos personales.[778] Esta disposición se inspira en el artículo 12, letra a), de la Directiva 95/46/CE, pero añade nuevos elementos para la información de los interesados relativos al periodo de conservación, sus derechos de rectificación, supresión o restricción y a presentar una reclamación.[779] Al igual que la Decisión Marco, el artículo 13 de la propuesta establece que los Estados Miembros podrán adoptar medidas legislativas que restrinjan el derecho de acceso, si así lo exige la naturaleza específica del tratamiento de datos en los ámbitos policial y de la justicia penal, y sobre la información del interesado relativa a una restricción de acceso, siguiendo en este punto al artículo 17, apartados 2 y 3, de la Decisión Marco 2008/977/JAI.[780]

---

[777] Artículo 17.3 de la Decisión Marco 2008/977/JAI.

[778] Esta obligación de garantizar el derecho de acceso, se da en dos fases. En la primera, «Los Estados Miembros reconocerán el derecho del interesado a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen». Sólo en caso que se confirme el tratamiento, surge la obligación del responsable de facilitará la siguiente información: « a) los fines del tratamiento; b) las categorías de datos personales de que se trate; c) los destinatarios o las categorías de destinatarios a quienes se han comunicado los datos personales, en particular los destinatarios establecidos en terceros países; d) el plazo durante el cual se conservarán los datos personales; e) la existencia del derecho a solicitar del responsable del tratamiento la rectificación, supresión o limitación del tratamiento de datos personales relativos al interesado; f) el derecho a presentar una reclamación ante la autoridad de control y los datos de contacto de la misma; g) la comunicación de los datos personales objeto de tratamiento, así como cualquier información disponible sobre su origen». Cfr. artículo 12.1 de la propuesta de Directiva.

[779] Cfr. COM (2012) 10 final, de 25.1.2012, p. 10.

[780] Ídem. La propuesta de Directiva de 2012, también regula la información que se debe entregar al interesado en caso que se niegue el derecho a acceder a si información personal. Al respecto el artículo 14 dispone que, cuando se restrinja el acceso directo, el interesado debe ser informado de la posibilidad de recurrir al acceso indirecto a través de la autoridad de control, que debe ejercer el derecho en su nombre y ha de informar al interesado del resultado de sus verificaciones. Por otro lado, el artículo 45 establece la obligación de los Estados Miembros de disponer las funciones de la autoridad de control, especialmente la admisión a trámite y la investigación de las reclamaciones y el fomento de la sensibilización de la

Por último, cabe consignar que el derecho de acceso también se encuentra reconocido en el Sistema de Información Schengen (SIS).[781] La persona interesada puede ejercer este derecho ante cualquiera de las autoridades competentes de los países que integran el SIS.[782] No obstante, el procedimiento para el ejercicio del derecho de acceso se rige por las normas del Estado ante el cual se ejerció el derecho. Lo anterior no es baladí si consideramos que las normas de procedimiento difieren de un país a otro, y más aún, en algunos países el derecho de acceso es directo y en otros, indirecto.[783] Por último, al igual toda la normativa sobre protección de datos, el SIS también contempla la posibilidad de que pueda restringirse o denegarse el derecho de acceso en caso que la entrega de dicha información sea perjudicial para la ejecución de algunas de las tareas en ella consignadas, o que dicha entrega de información afecte derechos y libertades de terceros.[784]

Como se puede apreciar, el derecho de acceso se ha ido perfeccionando con el correr del tiempo en el sistema europeo. En principio este derecho sólo contemplaba la facultad del interesado para requerir al responsable información relativa a la existencia de un fichero y su finalidad, así como la identidad del responsable del mismo. Ahora, se han ido agregando el objeto de tratamiento, así como el origen de dichos datos y a los

---

opinión pública sobre riesgos, normas, garantías y derechos. Cuando se deniegue o restrinja el acceso directo, una función propia de las autoridades de control en el contexto de la presente Directiva es el ejercicio del derecho de acceso por cuenta de los interesados y de verificación de la licitud del tratamiento de datos. Por último, el considerando 35 de la propuesta señala que «Cuando los Estados Miembros hayan adoptado medidas legislativas que restrinjan, total o parcialmente, el derecho de acceso, el interesado debe tener derecho a solicitar que la autoridad nacional de control competente verifique la licitud del tratamiento. El interesado debe ser informado de este derecho. Cuando el acceso sea ejercido por la autoridad de control por cuenta del interesado, este debe ser informado por la autoridad de control, como mínimo, de que se han llevado a cabo las verificaciones necesarias y del resultado en cuanto a la licitud del tratamiento en cuestión». Cfr. Exposición detallada de la propuesta de Directiva, COM(2012) 10 final, de 25.1.2012, p. 9 y 12.

[781] Artículo 109 del Convenio de Schengen de 1990. Las Autoridades de Control Común de Schengen, elaboraron en el año 2009, una guía para el ejercicio de este derecho. Cfr. *Data protection Secretary – A Guide for excercising the right of acces – 13 October 2009.*

[782] Esta facultad de elección para el titular de los datos respecto de la autoridad ante la cual ejerce su derecho, es posible porque las bases de datos nacionales (N.SIS) son idénticas a las del sistema central (C.SIS). Cfr. artículo 92.2 del Convenio Schengen.

[783] El derecho de acceso será «directo» si el interesado se puede dirigir directamente ante las autoridades que tratan los datos y obtener respuesta de las mismas, en cambio, será «indirecto», si la personas interesada deben presentar su solicitud para ejercer el derecho de acceso ante la Agencia nacional de protección de datos del Estado donde presenta la solicitud y es la agencias, la que comprueba el dato introducido en el SIS y le responde al interesado. Para ver los procedimientos y criterior específicos de cada Estado, véase *Data protection Secretary – A Guide for excercising the right of acces – 13 October 2009.*

[784] Artículo 109.2 del Convenio Schengen de 1990

destinatarios o las categorías de destinatarios a quienes se comuniquen o pretendan comunicar dichos datos. Por último, creemos que en el ámbito específico de la protección y represión penal, las limitaciones y excepciones a este derecho son reguladas de manera bastante generosa, lo que es atendible por la finalidad que se persigue con el tratamiento, pero pone en riesgo el real equilibrio entre los dos valores en juego, la libertad y la seguridad, balanceando la misma en favor de éste último.

2.3. Derecho de rectificación

El derecho de rectificación permite al interesado solicitar a la persona responsable del fichero la corrección de los datos de carácter personal que pudieran resultar incompletos o inexactos.[785] Generalmente, este derecho será puesto en ejercicio con posterioridad al derecho de acceso, ya que sólo una vez ejercido éste derecho, la persona estará en condiciones de saber si los datos tratados son inexactos o incompletos. El derecho de rectificación se encuentra estrechamente ligado con el principio de calidad o veracidad de los datos, ya que ambos persiguen que el tratamiento sea un fiel reflejo de la realidad.[786]

El reconocimiento del derecho de rectificación lo podemos rastrear en el sistema supranacional europeo hasta el Convenio 108 de 1981, donde se le reconoce como una garantía complementaria para la persona concernida, facultando a la misma para solicitar la rectificación de dichos datos «cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio».[787] Con posterioridad, en el ámbito específico de la cooperación policial, la Recomendación 87 (15) del Consejo de Europa, reconoce como un principio del tratamiento que el interesado sea capaz de obtener,

[785] Resolución de Madrid, relativa a *estándares internacionales sobre protección de datos personales y privacidad*, adoptada por la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad de 5.11.2009, p. 19.
[786] Javier APARICIO SALOM. *Estudio sobre la ley orgánica de protección de datos de carácter personal*. 3º edición. Pamplona: Aranadi, 2009, p. 254; GUERRERO PICÓ, *El Impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, p. 299.
[787] Artículo 8, letra c) del Convenio 108 de 1981.

cuando proceda, la rectificación de sus datos que se encuentren contenidos en un archivo.[788]

En el Derecho de la Unión Europea, también se reconoce esta facultad para la persona interesada. Primero en la Directiva general 95/46/CE[789], luego en la Carta de Derechos Fundamentales de la Unión Europea, donde se reconoce expresamente el derecho de rectificación de los datos personales al titular de los mismos.[790] Por su parte, la Decisión Marco 2008/977/JAI también reconoce el derecho a rectificación al titular de los datos personales, pero de una manera bastante particular. Primero lo consagra como una obligación del responsable del tratamiento de velar porque los datos sean correctos. Para ello la autoridad **podrá** rectificar los datos cuando sean incorrectos y, cuando sea posible y necesario, completarlos o actualizarlos.[791] De la lectura del artículo 4.1 de la Decisión Marco, queda la impresión de que es una facultad y no una obligación para la autoridad policial o judicial que trata los datos el rectificar los mismos cuando sean incorrectos, lo que atenta contra la propia naturaleza del tratamiento, ya que estos deben ser rectificados y monitoreados periódicamente dada la naturaleza y finalidad de este tipo de tratamiento. Además, al dejar la regulación del ejercicio de este derecho a lo dispuesto por la legislación de cada Estado de la Unión, las diferencias en cuanto a la efectividad del derecho pueden ser considerables.[792]

La propuesta de Directiva sobre protección de datos en el ámbito de la prevención y represión penal, al igual que la Decisión Marco, reconoce la rectificación

[788] Principio 6. *La publicidad, derecho de acceso a los archivos de la policía, el derecho de rectificación y derecho de los recursos de casación*, en particular véase el número 6.3.

[789] Artículo 12 b) de la Directiva 95/46/CE. La propuesta de Reglamento General de Protección de Datos Personales, destina un artículo en particular a regular el derecho de rectificación, en los siguientes términos: «artículo 16 *Derecho de rectificación.* El interesado tendrá derecho a obtener del responsable del tratamiento la rectificación de los datos personales que le conciernen cuando tales datos resulten inexactos. El interesado tendrá derecho a que se completen los datos personales cuando estos resulten incompletos, en particular mediante una declaración rectificativa adicional.» Cfr. COM (2012) 11 final, de 25.1.2012.

[790] Artículo 8 CDFUE.

[791] Artículo 4.1. de la Decisión Marco 2008/977/JAI.

[792] Al respecto, el considerando 15 de la Decisión Marco, dispone: «Por lo que respecta a los datos inexactos, incompletos o anticuados transmitidos a otros Estados Miembros o puestos a su disposición y tratados a continuación por autoridades cuasi judiciales —entendiéndose por tales las autoridades competentes para adoptar resoluciones jurídicamente vinculantes—, su rectificación, supresión o bloqueo debe efectuarse con arreglo al Derecho nacional». Sobre el derecho de rectificación en el derecho español, véase María del Carmen GUERRERO PICÓ, *El Impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, pp. 298-300; Marpia Mercedes SERRANO PÉREZ, *El derecho fundamental a la protección de datos. Derecho español y comparado*, pp. 357-365; y Javier APARICIO SALOM, *Estudio sobre la ley orgánica de protección de datos de carácter personal*.

como un derecho del titular de los datos, pero también como una obligación del Estado que trata los datos. En este último sentido, la propuesta impone al Estado miembro velar por que el responsable del tratamiento «tome todas las medidas oportunas para facilitar al interesado, al menos, la siguiente información: d) la existencia del derecho a solicitar del responsable del tratamiento el acceso a los datos personales relativos al interesado y su **rectificación**, su supresión o la limitación de su tratamiento».[793] Por tanto, la propuesta de Directiva lo primero que hace es regular la obligación del Estado de informar al titular de los datos, entre otros extremos, del derecho a la rectificación.

Otra obligación para los Estados contemplada la propuesta de Directiva, en relación al derecho de rectificación, es que el responsable del tratamiento informe por escrito al interesado sobre cualquier denegación de rectificación, sobre las razones de la denegación, y sobre las posibilidades de presentar una reclamación ante la autoridad de control y de interponer un recurso judicial.[794] Lo anterior está inspirado en el artículo 18, apartado 1, de la Decisión Marco 2008/977/JAI.[795]

Por otra parte, la propuesta de Directiva también contempla la rectificación como un derecho en favor del titular de los datos en los siguientes términos: «Los Estados Miembros reconocerán el derecho del interesado a obtener del responsable del tratamiento la rectificación de los datos personales que le conciernen cuando tales datos resulten inexactos».[796] Esta disposición está inspirada en el artículo 12, letra b), de la Directiva 95/46/CE.[797]

Por último, la propuesta de Directiva, al igual que la Decisión Marco, regula los derechos del interesado en las investigaciones y los procedimientos penales.[798] No obstante, la propuesta representa una evolución al respecto, ya que es mucho más precisa que la norma a derogar. Mientras el artículo 4.4. de la Decisión Marco se limita a señalar que «Si los datos personales forman parte de una resolución judicial o registro relacionado con el pronunciamiento de una resolución judicial, la rectificación,

[793] Artículo 11.1 de la Propuesta de Directiva COM (2012) 10 final.
[794] Artículo 15.2 de la Propuesta de Directiva COM (2012) 10 final.
[795] Propuesta de Directiva COM (2012) 10 final, p. 9.
[796] Artículo 15.1 de la Propuesta de Directiva COM (2012) 10 final.
[797] Propuesta de Directiva COM (2012) 10 final, p. 9.
[798] Artículo 4.4 de la Decisión Marco 2008/977/JAI y 17 de la Propuesta de Directiva COM (2012) 10 final.

supresión o bloqueo se efectuará de conformidad con la normativa nacional sobre procedimientos judiciales», la propuesta de Directiva, en su artículo 17, precisa que «Los Estados Miembros dispondrán que los derechos de información, acceso, rectificación, supresión y limitación del tratamiento contemplados en los artículos 11 a 16 se ejercerán de conformidad con las normas nacionales de enjuiciamiento cuando los datos personales figuren en una resolución judicial o en un registro tratado en el curso de investigaciones y procedimientos penales».[799] Como se puede apreciar, en ambos cuerpos normativos se remite a la legislación nacional para regular este derecho cuando los datos sean tratados con fines de investigación y represión penal. Tal como hemos venido sosteniendo, tal situación puede generar disparidad de criterios de un Estado a otro en cuanto a la forma como se regula el ejercicio del derecho. Por tanto, creemos que al momento de evaluar la aplicación de la normativa se debería intentar una reforma que permita homogenizar criterios al respecto, ya que por la vía de normas especiales en los procedimientos de enjuiciamiento penal, se podría crear una brecha de excepciones que haga ilusorio, ya no sólo del derecho de rectificación sino del ejercicio de las facultades que emanan del derecho a la protección de datos en su totalidad.[800]

2.4. Derecho de oposición, supresión (cancelación) y bloqueo

El derecho de oposición faculta a la persona interesada para impedir el tratamiento de sus datos de carácter personal cuando concurra una razón legítima derivada de su concreta situación personal.[801] La oposición supone que el tratamiento de

[799] El considerando 36 de la propuesta de Directiva refuerza esta idea al señalar: «Toda persona debe tener derecho a que se rectifiquen los datos personales inexactos que le conciernan y a que se supriman, cuando el tratamiento de estos datos no cumpla los principios esenciales establecidos en la presente Directiva. *Cuando los datos personales se sometan a tratamiento en el transcurso de investigaciones y procedimientos penales, los derechos de información, acceso, rectificación, supresión y restricción del tratamiento pueden ejercerse de conformidad con las normas nacionales relativas a los procedimientos judiciales*» [el destacado es nuestro].

[800] Manifestación de lo señalado es el considerado 82 de la propuesta de Directiva, que dispone que la misma «no impedirá que los Estados Miembros regulen el ejercicio de los derechos de los interesados sobre información, acceso, rectificación, supresión y restricción de sus datos personales tratados en el marco de un procedimiento penal, y sus posibles restricciones, en las normas nacionales en materia de enjuiciamiento penal».

[801] En esta línea el derecho de oposición ha sido definido por Sánchez Bravo como «como el derecho del interesado a negarse, por motivos legítimos, a que sus datos personales sean objeto de tratamiento». Cfr. Álvaro SÁNCHEZ BRAVO, *La protección del derecho a la libertad informática en la Unión Europea*, p. 97. En la misma línea véase la Resolución de Madrid, relativa a *estándares internacionales sobre protección de datos personales y privacidad*, adoptada por la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad de 5.11.2009, principio 18.

los datos aún no se ha realizado, ya que en este último caso lo que procedería sería ejercer el derecho de cancelación.[802]

El derecho de oposición no se encuentra expresamente reconocido ni en el Convenio 108 del Consejo de Europa ni en la Carta de Derecho Fundamentales de la Unión Europea.[803] Este derecho tuvo su origen en la Ley francesa, es decir, con anterioridad a la aprobación de la Directiva 95/46/CE.[804] No obstante, será dicha Directiva la primera norma supranacional europea que reconoce y regula el derecho de oposición como tal.[805] Lo anterior contrasta con la regulación en materia tratamiento de datos en el ámbito de la cooperación policial y judicial, dónde no existe ninguna disposición ni referencia al derecho de oposición. Ello es así, porque en principio, el interesado, cuyos datos están siendo tratados con fines de prevención y represión penal, no podría oponerse a dicho tratamiento siempre que el mismo se realice por la autoridad policial o judicial competente de cada Estado en el ámbito de sus atribuciones.[806]

[802] El derecho de oposición se encuentra estrechamente vinculado a los tratamientos automatizados de datos personales. Cfr. Resolución de Madrid, principio 18.3, p. 20.

[803] No obstante, esta falta de reconocimiento expreso, el TJCE, partiendo del reconocimiento al derecho a la vida, a reconocido al titular de los datos a que cierta información de carácter personal sea conocida. Cfr. STJCE de 5 de octubre de 1994, caso *X. vs. Comisión*, en la que ante un posible contrato de trabajo, el interesado se oponía a cualquier tipo de prueba médica que permitiera sospechar o comprobar la existencia del virus VIH. Al respecto véase, Mónica ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*. Valencia: Tirant lo Blanch, 2006, p. 263.

[804] Mónica ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, p. 499. Sobre el derecho de oposición en la legislación española véase María Mercedes SERRANO PÉREZ, *El derecho fundamental a la protección de datos. Derecho español y comparado*. Madrid: Civitas, 2003, pp. 369-373 María del Carmen GUERRERO PICÓ, *El Impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal.* Thomson-Civitas, 2006, pp. 303-308; Javier APARICIO SALOM, *Estudio sobre la ley orgánica de protección de datos de carácter personal*. 3º edición. Pamplona: Aranzadi, 2009, pp. 257-260.

[805] El artículo 14 de la Directiva 95/46/CE reconoce dos supuesto para que proceda el derecho de oposición: a) Por razones legítimas vinculadas a su situación personal; y b) en casos de tratamiento destinados a la prospección comercial. El Artículo 13 de la Directiva 2002/58/CE sobre Protección de Datos y Comunicaciones Electrónicas, también ofrece la posibilidad al abonado del servicio de oponerse a recibir comunicaciones electrónicas no solicitadas. También, cabe tener presente que basado en este mismo artículo de la Directiva 95/46/CE, pero con algunas modificaciones, especialmente por lo que respecta a la carga de la prueba y su aplicación a la mercadotecnia directa, el artículo 19 de la propuesta de Reglamento General sobre Protección de Datos, establece también el derecho de oposición del interesado. Cfr. COM(2012) 11 final, de 25.1.2012, p. 10.

[806] Al respecto, la resolución de Madrid, contempla la posibilidad de restringir el ejercicio de este derecho en «aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación impuesta sobre la persona responsable por la legislación nacional aplicable». Cfr. principio 18.2 de Resolución de Madrid, *relativa a estándares internacionales sobre protección de datos personales y privacidad*, adoptada por la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad de 5.11.2009, p. 20.

Otra de las facultades inherentes a la protección de los datos personales es el derecho de supresión, cancelación o borrado de los datos. Este derecho supone la realización previa de un tratamiento de los datos personales, ya que si no ha procedido aún el tratamiento, el derecho que correspondería ejercer sería el derecho de oposición. Por otra parte, si los datos tratados son inexactos o incompletos, ello no da necesariamente origen a la cancelación de los datos, sino de la rectificación de los mismos. Por tanto, estaremos en presencia del ejercicio del derecho de supresión, cuando el tratamiento de los datos personales carezca de una base de legitimación, es decir, cuando no exista un consentimiento por parte del titular de los datos, ni una habilitación legal para el tratamiento de los datos.[807]

En el ámbito del Consejo de Europa, el Convenio 108, se refiere a esta facultad del titular de los datos como una garantía en favor del titular de los datos para «**borrar**» los datos personales, cuando el tratamiento se haya efectuado en contravención a los principios en ella consagrados.[808] Por su parte, la Recomendación 87 (15) del Consejo de Europa, referida al tratamiento de datos con fines policiales, consagra, por una parte, que los datos deben ser eliminados en el caso que se consideren excesivos, inexactos o irrelevantes en la aplicación de cualquiera de los otros principios contenidos en la presente Recomendación; y por otra, que dicha supresión se deben extender en la medida de lo posible a todos los documentos que acompañan al expediente de la policía y, si no se realiza inmediatamente, debe llevarse a cabo, a más tardar en el momento de la transferencia posterior de los datos o de su próxima comunicación.[809]

Por otro lado, la CDFUE no realiza una referencia expresa al derecho de cancelación, no obstante, el mismo se debe entender incluido también en el derecho a la

[807] Desde un punto de vista analítico cercano al derecho civil, Javier Aparicio, ha definido el derecho de cancelación (en base a la LOPD) como «el derecho del interesado a que excluyan del tratamiento datos de carácter personal, ya sea por ser erróneos, o por no interesarle [al interesado] que se sometan a tratamiento». Cfr. Javier APARICIO SALOM, *Estudio sobre la ley orgánica de protección de datos de carácter personal.* 3º edición. Pamplona: Aranzadi, 2009, p. 254. No compartimos dicha definición, pues el primer supuesto, esto es, el de los datos erróneos, creemos que en dicha hipótesis es propio el ejercicio del derecho de rectificación, y en caso de no interesarle a la persona afectada que se traten sus datos, antes que se inicie el tratamiento de sus datos, creemos que en dicho caso estamos en presencia del derecho de oposición más que de cancelación. En todo caso, como veremos más adelante, en el ámbito de la prevención y represión penal, este derecho más que partir de la base del consentimiento del titular de los datos, lo hace sobre la base de la habilitación legal previa para realizar el tratamiento, por lo que la lógica civilista se ve bastante mermada para dar solución a los problemas que se nos presentan.
[808] Artículo 8 del Convenio 108 del Consejo de Europa.
[809] Principio 6.3., apartado dos y tres de la Recomendación 87 (15) del Consejo de Europa.

protección de datos, de lo contrario este quedaría trunco. Donde sí se reconoce expresamente es en las Directivas comunitarias sobre Protección de Datos.[810] La propuesta de Reglamento General de Protección de Datos de 2012, en su artículo 17, establece y regula el derecho del interesado al olvido y supresión.[811] Asimismo elabora y especifica este último derecho, que se establece en el artículo 12, letra b), de la Directiva 95/46/CE y norma las condiciones del derecho al olvido, incluida la obligación del responsable del tratamiento que haya difundido los datos personales, de informar a los terceros sobre la solicitud del interesado de suprimir todos los enlaces a los datos personales, copias o réplicas de los mismos. También integra el derecho a que se **restrinja** el tratamiento en determinados casos, evitando la ambigüedad del término «bloqueo».[812]

En el ámbito específico de la protección de datos en materia de cooperación policial y judicial, la Decisión Marco 2008/977/JAI, establece que «los datos personales se suprimirán o disociarán cuando ya no sean necesarios a los fines para los que fueron legalmente recogidos o legalmente tratados posteriormente».[813] No obstante, esta disposición no se aplica a los archivos de datos contenidos en conjuntos independientes de datos durante un período adecuado de tiempo realizado de acuerdo con el Derecho nacional.[814] Esta disposición nos genera varias interrogantes, de partida, ¿qué se entiende por conjunto independiente de datos? Y por otra parte ¿cuánto es un periodo adecuado de tiempo? El primer interrogante, podría referirse a algún tipo particular de sospechoso o autor de un delito, o algún medio de prueba respecto del cual se quiera

[810] El Artículo 12 de la Directiva 95/46/CE consagra, a propósito del derecho de acceso que «Los Estados Miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento: b) en su caso, la rectificación, la **supresión** o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos» [el destacado en nuestro].

[811] Artículo 17 **Derecho al olvido y a la supresión**. «1. El interesado tendrá derecho a que el responsable del tratamiento *suprima* los datos personales que le conciernen y se abstenga de darles más difusión, especialmente en lo que respecta a los datos personales proporcionados por el interesado siendo niño, cuando concurra alguna de las circunstancias siguientes: a) los datos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados; b) el interesado retira el consentimiento en que se basa el tratamiento de conformidad con lo dispuesto en el artículo 6, apartado 1, letra a), o ha expirado el plazo de conservación autorizado y no existe otro fundamento jurídico para el tratamiento de los datos; c) el interesado se opone al tratamiento de datos personales con arreglo a lo dispuesto en el artículo 19; d) el tratamiento de datos no es conforme con el presente Reglamento por otros motivos». [el desatacado es nuestro]. La propuesta también hace referencia al derecho a la supresión en el considerando 53. Cfr. COM (2012) 11 final.

[812] Cfr. COM (2012) 11 final, p. 10.

[813] Artículo 4.2. de la Decisión Marco 2008/977/JAI.

[814] Ídem.

mantener los datos personales por un periodo superior al que excede una investigación o juicio concreto. Por otra parte, un periodo «adecuado» de tiempo no significa que dichos datos queden guardado por un lapso superior al necesario para la consecución de los fines de prevención o represión penal, por tanto, postulamos al respecto que dicho plazo no podría exceder el tiempo necesario para que se aplique la prescripción de los delitos perseguidos.[815]

En la nueva propuesta de Directiva sobre protección de datos en el ámbito de la prevención y represión penal, se destina el artículo 16 a regular el derecho de supresión. Dicho artículo se inspira en el artículo 12, letra b), de la Directiva 95/46/CE y, por lo que se refiere a las obligaciones en caso de denegación, en el artículo 18, apartado 1, de la Decisión Marco 2008/977/JAI.[816]

En el caso que los datos tratados formen parte de una resolución judicial o registro relacionado con el pronunciamiento de una resolución judicial, la rectificación, supresión o bloqueo se efectuará de conformidad con la normativa nacional sobre procedimientos judiciales, es decir, en tal caso, rige la norma interna de cada país.[817]

La propuesta de Directiva, también incluye la posibilidad de «marcar» los datos, en lugar de proceder a la supresión en tres supuestos, que: a) el interesado impugne su exactitud, durante un plazo que permita al responsable del tratamiento verificar la exactitud de dichos datos; b) los datos personales hayan de conservarse a efectos probatorios; c) el interesado se oponga a su supresión y solicite la limitación de su uso.[818]

Por último, junto con el derecho a suprimir, cancelar o eliminar los datos, la propuesta de Directiva contempla la obligación de los Estados Miembros de obligar a

[815] Este punto se encuentra estrechamente vinculado al derecho al olvido. Este no se ha desarrollado tanto el ámbito de la prevención y represión penal como sí lo ha hecho en el ámbito del derecho comunitario.
[816] COM(2012) 10 final, p. 9
[817] Artículo 4.4. de la Decisión Marco 2008/977/JAI. Un tema estrechamente vinculado es la accesibilidad *on line* a los expediente judiciales, y en concreto, si se debe articularse como un sistema cerrado con alcance sólo a las partes del procedimiento o a quienes tengan un interés legítimo en él, o por el contrario, como un sistema abierto al público en general. Al respecto véase Corazón MIRA ROS, "Algunas reflexiones sobre la protección de datos personales en el ámbito judicial", en *Actas del IV Congreso Gallego de Derecho Procesal* (Universidad da Coruña, 2012), pp. 581–94.
[818] Artículo 16.3 de la propuesta de Directiva COM (2012) 10 final.

los responsables del tratamiento a informar por escrito al interesado de cualquier denegación de la supresión o marcado del tratamiento, las razones de la denegación y las posibilidades de presentar una reclamación ante la autoridad de control, y de interponer un recurso judicial.[819]

Otra facultad incluida en el derecho a la protección de datos personales, es la posibilidad de solicitar, por parte del interesado, el **bloqueo de los datos**. Este derecho al bloqueo es una novedad introducida por la Directiva comunitaria 95/46/CE, ya que el Convenio 108 sobre Protección de Datos del Consejo de Europa no la contempla.[820] Para algunos autores, el derecho al bloqueo procede para aquellos supuestos en los que es necesario paralizar el tratamiento de los datos, pero en que no es posible la supresión de estos.[821]

En el ámbito de la prevención o represión penal, el «bloqueo» se ha definido como la señalización o marcado de datos personales conservados con el objetivo de limitar su tratamiento en el futuro.[822] La Decisión Marco 2008/977/JAI señala que los datos personales se bloquearán, en lugar de suprimirse, en caso de que haya razones justificadas para suponer que la supresión pueda perjudicar los intereses legítimos del interesado.[823] En tal caso, los datos bloqueados podrán tratarse solo para los fines que impidieron su supresión.[824] No obstante, la propuesta de Directiva de protección de datos en el ámbito de la prevención y represión penal de enero de 2012, elimina el concepto de bloqueo de datos por considerarlo *ambiguo*, y en su reemplazo establece la «**restricción de tratamiento**», definiéndolo como el marcado de los datos de carácter personal, conservados con el fin de limitar su tratamiento en el futuro.[825] Como se puede apreciar, tanto el bloqueo como el marcado de los datos tienen por finalidad

[819] Artículo 16.4 de la propuesta de Directiva COM (2012) 10 final.
[820] Artículo 12 b) y c) de la Directiva 95/46/CE. Si bien, la Directiva hace referencia al «bloqueo» como un derecho del interesado en caso que el tratamiento no se ajuste a sus disposiciones, y particularmente, en caso que los datos sean incompleto o inexacto, no define que se debe entender por bloqueo ni en que consiste el ejercicio de dicho derecho.
[821] Mónica ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, p. 306
[822] Artículo 2 c) y 18, apartado 1, de la Decisión Marco 2008/977/JAI; artículo 24.1 e) de la Decisión 2008/615/JAI.
[823] Artículo 4.3 de la Decisión Marco 2008/977/JAI.
[824] Ídem.
[825] Artículo 3.4, de la Propuesta de Directiva COM (2012) 10 final, de 25.1.2012, p. 28.

limitar el uso de los datos única y exclusivamente para los fines que impidieron su supresión.

Ahora bien, el derecho al bloqueo o marcado, entendido como una restricción al uso de los datos, se reconoce no sólo al titular de los datos sino también a los Estados Miembros o autoridades encargadas del tratamiento de dichos datos, como ocurre por ejemplo, en el SIS, en el SIA, en Eurodac, Europol y Eurojust.[826]

El bloqueo o marcado de los datos apuntan en definitiva a lo mismo: **abstraer** los datos del tratamiento original que validó su uso y **limitarlo** sólo para dar cumplimiento al nuevo fin, que generalmente dirá relación con el ejercicio de los derechos de la persona interesada. Pensemos por ejemplo, en el caso de que una persona tome conocimiento que sus datos están siendo tratados con fines policiales por ser considerado sospechoso de la comisión de un ilícito. Luego de acreditado que no tuvo ninguna participación en los hechos, quiere interponer un reclamo ante la autoridad de control o un recurso para ante los tribunales con la finalidad de perseguir responsabilidades respecto del ente persecutor, por considerar que fue objeto de una imputación falsa. En tal caso, podría solicitar que sus datos, que constan en las bases de la policía, sean bloqueados o marcados con el doble fin de saber cuáles son los datos personales que fueron tratados, por qué y para qué, y por otra parte, para impedir que dichos datos sean suprimidos o cancelados antes de que pueda ejercer alguna acción al respecto. Cabe recordar al respecto, que el responsable del tratamiento debe informar por escrito al interesado de cualquier denegación de la supresión o marcado del tratamiento, las razones de la denegación y las posibilidades de presentar una reclamación ante la autoridad de control y de interponer un recurso judicial.[827]

Por último, si los datos personales forman parte de una resolución judicial o registro relacionado con el pronunciamiento de una resolución judicial, el bloqueo o marcado se efectuará de conformidad con la normativa nacional sobre procedimientos

[826] Cfr. artículo 101 Convenio Schengen; artículo 7 del Convenio SIA; artículo 15 del Reglamento Eurodac; artículos 9 y 10 Convenio Europol; y artículo 18 Decisión Eurojust. Al respecto, véase Mónica ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, pp. 306-307.

[827] Artículo 18.1 de la Decisión Marco 2008/977/JAI; y artículo 16.4 de la propuesta de Directiva COM (2012) 10 final.

judiciales.[828] La propuesta de Directiva aclara el punto sobre qué se debe entender por «registro relacionado con el pronunciamiento de una resolución judicial», al señalar derechamente que se trata de registros tratados en el curso de investigaciones y procedimientos penales, es decir, consagra el derecho al bloqueo o marcado tanto en las investigaciones como en los procedimientos penales.[829]

2.5. Derecho a presentar un recurso

Para el caso que los derechos del interesado no sean respetados, la mayoría de la legislación sobre protección de datos contempla la facultad del interesado de interponer recursos.[830] Este derecho tiene como supuesto habilitante para su ejercicio, que no se haya respetado previamente las disposiciones sobre protección de datos, como por ejemplo el derecho a la información, de acceso, de rectificación o supresión, o bien, las normas sobre transferencia internacional de datos.

La facultad de interponer un recurso es un *derecho* del interesado, pero también una *obligación* para los Estados Miembros de la Unión.[831] Éstos deben establecer y reconocer que toda persona disponga de un recurso judicial, en caso de violación de los derechos, que le garanticen las disposiciones de Derecho nacional aplicables al tratamiento de que corresponda.[832] En el caso específico del tratamiento de datos con fines de prevención y represión penal, la propuesta de Directiva de 2012 es mucho más explícita que la Decisión Marco 2008/977/JAI respecto de la obligación de los Estados Miembros de reconocer el derecho que asiste a todo interesado a presentar una

[828] Artículo 4.4. de la Decisión Marco 2008/977/JAI.
[829] Artículo 17 de la propuesta de Directiva COM (2012) 10 final.
[830] Cfr. Artículo 8 y 10 del Convenio 108 de 1981; Principio nº 6 de la Recomendación 87(15) del Consejo de Europa; artículo 22 y 28.3 de la Directiva 95/46/CE; artículos 73 a 75 de la propuesta de Reglamento General sobre Protección de Datos, COM (2012) 11 final; artículos 18.1, 20 y 25.2 de la Decisión Marco 2008/977/JAI; y artículos 50 a 52 de la propuesta de Directiva COM (2012) 10 final. No obstante, algunas normas sobre tratamiento de datos personales en actividades específicas de prevención y represión penal, como por ejemplo el Tratado de Prüm y la Decisión 2008/615/JAI que integra al ordenamiento jurídica de la Unión Europea dicho acuerdo, no contempla ninguna referencia a la facultad de los titulares de los datos de recurrir ante las autoridades de control o jurisdiccionales en caso de vulneración de los derechos inherentes a la protección de datos personales.
[831] El principio de responsabilidad de los Estados también se encuentra en la Resolución de Madrid, en los siguientes términos: Principio 25.2. «Los Estados promoverán las medidas adecuadas para facilitar el acceso de los interesados a los correspondientes procesos, judiciales o administrativos, que les permitan obtener la reparación de los daños y/o perjuicios anteriormente mencionados». *Estándares internacionales sobre protección de datos personales y privacidad*, adoptada por la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, Madrid, 5.11.2009, p. 27.
[832] Artículo 22 de la Directiva 95/46/CE.

reclamación ante la autoridad de control de cualquier Estado miembro, si considera que el tratamiento de sus datos personales no se ajusta a las disposiciones de las Directivas europeas.[833] La Decisión Marco se limita a reconocer el derecho del interesado a un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables. En cambio, la propuesta señala que el derecho a reclamar le asiste a todo interesado si considera que el tratamiento de sus datos personales no se ajusta a las disposiciones de la Directiva europea.[834]

Ante la vulneración de la normativa específica sobre protección de datos, el interesado tiene la opción de ocurrir ante la autoridad administrativa encargada de velar por el cumplimiento de la misma, por medio de una «**reclamación**», o acudir directamente a los Tribunales ordinarios de justicia competentes de acuerdo a las reglas de cada Estado e interponer un «**recurso judicial**». De esta forma, el interesado, si considera que se vulneran sus derechos en el marco de las disposiciones sobre protección de datos, facultativamente puede presentar una reclamación ante una autoridad de control o presentar un recurso judicial. Por tanto, no es requisito previo para interponer una acción judicial el haber presentado una reclamación ante la autoridad administrativa encargada de velar por el cumplimiento de la protección de datos.[835]

En lo referido al derecho a presentar una reclamación ante una autoridad de control, la propuesta de Directiva de 2012 establece la posibilidad de que el interesado pueda presentar su reclamación ante la autoridad de control **de cualquier Estado miembro** (artículo 50.1).[836] Éste artículo está inspirado en el artículo 28, apartado 4, de la Directiva 95/46/CE y se refiere a cualquier infracción de la Directiva en relación con el reclamante.[837] Cabe tener presente que también se puede presentar un recurso judicial contra la inactividad o dilación de una decisión por parte de las autoridades de control.

[833] Artículo 50.1 de la propuesta de Directiva COM (2012) 10 final, de 25.1.2012.
[834] Cfr. artículo 20 de la Decisión Marco 2008/977/JAI y artículo 50.1 de la propuesta de Directiva COM (2012) 10 final.
[835] Al respecto la Resolución de Madrid, dispone: «En todo caso, y sin perjuicio de los recursos administrativos ante las citadas autoridades de supervisión, incluyendo el control jurisdiccional de sus decisiones, el interesado podrá acudir directamente a la vía jurisdiccional para hacer valer sus derechos conforme a las previsiones establecidas en la legislación nacional aplicable». Cfr. Principio n° 25.3 de los *Estándares internacionales sobre protección de datos personales y privacidad*, adoptada por la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, Madrid, 5.11.2009, p. 25.
[836] En el mismo sentido, véase el Considerando 60 de la Propuesta de Directiva COM (2012) 10 final.
[837] Ibídem, p. 13.

La propuesta de Directiva reconoce al titular el derecho a reclamar en dos hipótesis: a) que la autoridad de control no haya dado curso a un reclamo (ausencia de una decisión) necesaria para proteger sus derechos, o b) en caso de que la autoridad de control no informe al interesado en el plazo de tres meses sobre el curso o el resultado de la reclamación, es decir, que exista una dilación injustificada. En ambos casos, la acción legal de reclamo debe interponerse ante los órganos jurisdiccionales del Estado en que este establecida la autoridad de control reclamada.[838]

Por otro lado, también asiste al interesado la **vía jurisdiccional** como derecho en dos momentos. El primero, cuando el titular de los datos recurre directamente a los tribunales una vez que se ha producido una vulneración a sus derechos por parte del responsable del tratamiento.[839] El segundo momento se da luego de presentar un recurso administrativo ante la autoridad de control correspondiente, y que este no se pronuncie o lo deseche. En tal caso, nace también para el titular de los datos el derecho a recurrir a los tribunales a reclamar la resolución de la autoridad de control, en caso que el interesado estime que dicha resolución es lesiva para sus derechos.[840] La propuesta de Directiva de 2012 sobre protección de datos en el ámbito de la prevención y represión penal es mucho más detallada que la Decisión Marco 2008/977/JAI en cuanto a los tipos de recursos a que tiene derecho el titular de los datos. Mientras la Decisión Marco, sólo destina el artículo 20 a regular lo que denomina vías de recurso[841], la propuesta de Directiva, en cambio, regula en tres artículos diferentes el derecho al recurso, distinguiendo entre: el derecho a presentar una reclamación ante una autoridad de control (artículo 50), el derecho a un recurso judicial contra una autoridad de control (artículo 51), y el derecho a un recurso judicial contra un responsable o encargado del tratamiento (artículo 52).

Por último, nos gustaría destacar dos ideas en relación al derecho al recurso por parte del interesado. La primera, dice relación con el desarrollo que ha tenido este derecho tanto en la propuesta de Reglamento General de Protección de datos como en la

[838] Artículo 51 de la Propuesta de Directiva COM (2012) 10 final, de 25.1.2012.
[839] Considerando 55 de la Directiva 95/46/CE.
[840] Artículo 28.3 parte final de la Directiva 95/46/CE.
[841] Artículo 20. *Vías de recurso*: «Sin perjuicio del recurso administrativo que pueda interponerse antes de acudir a la autoridad judicial, el interesado tendrá derecho a un **recurso judicial** en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables» [el destacado es nuestro].

propuesta de Directiva para el ámbito de la prevención y represión penal. En efecto, se pasa de una regulación mínima o básica a una regulación más detallada, distinguiendo si el recurso es de carácter administrativo o jurisdiccional. Además, se extiende el derecho a presentar una reclamación ante una autoridad de control en cualquier Estado miembro, y a presentar un recurso judicial si considera que se vulneran sus derechos en el marco de la presente Directiva o en caso de que la autoridad de control no reaccione ante una reclamación o no actúe cuando dicha medida sea necesaria para proteger los derechos del interesado.[842] También es importante destacar que el derecho a presentar un recurso se extiende tanto a las personas físicas como jurídicas, y particularmente, dentro de éstas últimas, a toda entidad, organización o asociación que tenga por objeto proteger los derechos e intereses de las personas en relación con la protección de sus datos.[843]

2.6. Derecho a ser indemnizado

Como criterio general, podemos señalar que todo interesado tiene derecho a ser indemnizado por los daños y/o perjuicios, tanto morales como materiales, que se le hubiesen causado como consecuencia de un tratamiento de datos de carácter personal que vulnere la legislación aplicable en materia protección de datos.[844] En el ámbito específico de la protección de datos personales con fines de prevención o represión penal, este tema se regula bajo los rótulos de «reparación», «responsabilidad» e «indemnización».[845]

---

[842] Considerando 60 de la propuesta de Directiva COM (2012) 10 final, de 25.1.2012

[843] Considerando 61 y 61 de la propuesta de Directiva COM (2012) 10 final, de 25.1.2012. Este es uno de los poco casos expresamente se hace extensiva a las personas jurídicas uno de los derechos propio de los interesados.

[844] Cfr. Principio n° 25.1 de la Resolución de Madrid sobre *Estándares internacionales sobre protección de datos personales y privacidad*, adoptada por la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, Madrid, 5.11.2009, p. 27. En el derecho español, el derecho de indemnización se encuentra regulado en el artículo 19 de la LOPD. Al respecto véase Javier APARICIO SALOM, *Estudio sobre la ley orgánica de protección de datos de carácter personal*, pp. 271-272; Mónica ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, pp. 350-351; María del Carmen GUERRERO PICÓ, *El Impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, pp. 308-310; María Mercedes SERRANO PÉREZ, *El derecho fundamental a la protección de datos. Derecho español y comparado*, pp. 376–377.

[845] Artículo 19 de la Decisión Marco 2008/977/JAI; Artículo 77 de la propuesta de Reglamento General de Protección de Datos COM (2012) 11 final; artículo 54 de la propuesta de Directiva COM (2012) 10 final, ambas de 25.1.2012. El Artículo 23 de la Directiva 95/46/CE regula a este tema bajo el término «responsabilidad». Tanto el Convenio 108 de 1981 como la Recomendación (87)15, ambas del Consejo de Europa, no contienen disposiciones particulares que regulan las indemnizaciones de los perjuicios causado, por lo que entendemos dejan dicho tema bajo el amparo de la legislación común aplicable en cada Estado en materia de responsabilidad en sus diversos ámbito: penal, civil y administrativa.

El artículo 54.1 de la propuesta de Directiva COM (2012) 10 final, establece como primera regla que «los Estados Miembros dispondrán que toda persona que haya sufrido un perjuicio como consecuencia de una operación de tratamiento ilícito o de un acto incompatible con las disposiciones adoptadas con arreglo a la presente Directiva tendrá derecho a recibir del responsable o encargado del tratamiento una indemnización por el perjuicio sufrido». Este artículo se inspira en los artículos 23 de la Directiva 95/46/CE y artículo 19, apartado 1, de la Decisión Marco 2008/977/JAI.[846]

A nuestro criterio, el derecho reconocido en el precepto citado comprende tanto la responsabilidad extracontractual o *aquiliana*, como la responsabilidad contractual, ya que sólo exige para que opere un tratamiento ilícito o actos incompatibles con lo preceptuado en la Directiva. En consecuencia, da lo mismo que la persona haya prestado previamente su consentimiento para el tratamiento; el titular de los datos siempre tendrá derecho a reclamar por el perjuicio sufrido. Hablamos entonces de una **responsabilidad objetiva**, es decir, que es necesario para que proceda, acreditar sólo la relación de causalidad entre un tratamiento y un daño, y asimismo, que dicho daño sea imputable al causante del mismo.

En caso de que participen en el tratamiento más de un responsable o encargado, la propuesta de Directiva señala que todos son **responsables solidarios** del importe total de los daños, ampliando este derecho a los perjuicios causados por los encargados del tratamiento y aclarando la responsabilidad de los corresponsables y coencargados.[847] De esta forma se supera la limitación de la Decisión Marco que sólo hacía referencia al responsable del tratamiento como sujeto responsable de los daños.[848]

[846] Propuesta de Directiva COM (2012) 9 final, de 25.1.2012, p. 13.
[847] Artículo 54.2 Propuesta de Directiva COM (2012) 9 final, de 25.1.2012, p. 13.
[848] Artículo 19.1 de la Decisión Marco 2998/977/JAI. Éste cuerpo legal, también señala una regla específica para determinar la responsabilidad en el caso de transferencias internacionales de datos, en los siguientes términos: «Si una autoridad competente de un Estado miembro transmitió datos personales, el destinatario no podrá, en el ámbito de sus responsabilidades ante la parte perjudicada de conformidad con el Derecho nacional, alegar en su defensa que los datos transmitidos eran inexactos. Si el destinatario repara los daños y perjuicios causados por el uso de datos inexactos transmitidos, la autoridad competente transmisora abonará al destinatario el importe pagado en concepto de daños y perjuicios, teniendo en cuenta cualquier responsabilidad que pueda imputarse al destinatario». Cfr. Artículo 19.2 de la Decisión Marco.

Por último, en la propuesta de Directiva se establece la posibilidad de que el responsable o el encargado del tratamiento puedan ser **eximidos** total o parcialmente de dicha responsabilidad si demuestran que no se les puede imputar el hecho que ha provocado el daño.[849]

3. LOS LÍMITES Y EXCEPCIONES AL EJERCICIO DE LOS DERECHOS

3.1. Consideraciones preliminares

El derecho a la protección de datos personales, como todo derecho fundamental, no es absoluto sino que puede ser objeto de injerencias, por la vía de las limitaciones o excepciones de las facultades que son inherentes. Estas injerencias emanan de la necesidad de compatibilizar su ejercicio con otros derechos, bienes y valores jurídicos susceptibles de protección, así como de su consideración en relación con su función en una sociedad democrática.[850] Ahora bien, dichas limitaciones no pueden ser arbitrarias, sino que deben cumplir con ciertos parámetros para que sean aceptadas como un acto legítimo de injerencia de un derecho fundamental.[851]

El reconocimiento y protección de los datos de carácter personal como derecho fundamental se encuentra en el artículo 16 del TFUE, en el artículo 8 del CEDH y en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea. La memoria explicativa de éste último instrumento señala que «cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Sólo se podrán introducir limitaciones, respetando el principio de proporcionalidad, 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».[852] Lo

[849] Artículo 54.3 Propuesta de Directiva COM (2012) 9 final, de 25.1.2012.
[850] Al respecto véase, Tribunal de Justicia de la Unión Europea, sentencia de 9.11.2010, asuntos acumulados C-92/09 y C-93/09 *Volker und Markus schecke y Eifert*.
[851] En concreto, dichas medidas, deben estar establecidas por ley, respetar el contenido esencial de dicho derecho y, respetando el principio de proporcionalidad, ser 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. Cfr. Artículo 52, apartado 1 de la CDFUE; y considerando 80 de la propuesta de Directiva COM (2012) 10 final.
[852] Artículo 52.1 de la CDFUE.

anterior se inspira en la jurisprudencia del Tribunal de Justicia, que ha establecido el criterio de que pueden establecerse restricciones al ejercicio de estos derechos, siempre que dichas restricciones respondan efectivamente a objetivos de interés general perseguidos por la comunidad y no constituyan, teniendo en cuenta el objetivo perseguido, una intervención desmesurada e intolerable que afecte a la esencia misma de dichos derechos.[853]

3.2. Regulación de los límites y excepciones en el tratamiento de datos con fines de prevención y represión penal

En el ámbito específico de la regulación de la protección de datos en materia de cooperación policial y judicial, la Decisión Marco 2008/977/JAI, a diferencia de la Directiva 95/46/CE, no destina un artículo específico a regular las excepciones y limitaciones al ejercicio de los derechos.[854] La Decisión Marco sólo contiene una disposición en la materia, destinada a normar el caso en que un Estado miembro transfiera datos personales a otro Estado miembro, y que dicha transferencia incluya datos que estén sometidos a alguna limitación especifica en el Estado transmisor. En tales casos, se impone la obligación al Estado transmitente de comunicar la limitación a la que estén sometidos los datos y no imponer más restricciones que las que contempla en su derecho interno. Por otro lado, a los Estados que reciben los datos, se le impone el deber respetar tales limitaciones.[855] En definitiva, se deja al derecho nacional de cada Estado determinar las correspondientes restricciones, ya sea de forma general o específica, por ejemplo, por ley o por medio de la publicación de una lista de las operaciones de tratamiento.[856]

Esta falta de regulación específica en materia de límites y excepciones al ejercicio de los derechos que integran la protección de datos por parte de la normativa europea, se mantiene en la propuesta de Directiva de 2012. En la propuesta que pretende derogar y reemplazar a la Decisión Marco 2008/977/JAI, sólo se regula específicamente

[853] Cfr. STJCE de 13 de abril de 2000, asunto C-292/97, considerando 45; y texto de las explicaciones relativas al texto completo de la Carta, en la versión que figura en el doc. CHARTE 4487/00 CONVENT 50.
[854] Artículo 13 de la Directiva 95/46/CE.
[855] Artículo 12 de la Decisión Marco 2008/977/JAI.
[856] Considerando 27 de la Decisión Marco 2008/977/JAI.

las limitaciones al derecho de acceso[857], distanciándose sobre este punto con la propuesta de Reglamento General de Protección de Datos, el cual es omnicomprensivo, en el sentido de que abarca todos los derechos del interesado, dejando que tanto el derecho nacional como el derecho de la Unión puedan establecer limitaciones al ejercicio de los derechos de información, acceso, rectificación y supresión.[858] La propuesta de Directiva, en cambio, entrega directamente a los Estados Miembros la regulación del ejercicio de todos los derechos de los interesados en las normas nacionales en materia de enjuiciamiento penal, salvo el caso citado del derecho de acceso, donde la propia Directiva establece los criterios para su limitación.[859]

Los criterios de limitación del derecho de acceso se encuentran detallados en el artículo 13 de la propuesta de Directiva COM (2012) 10 final, en los siguientes términos: «1. Los Estados Miembros podrán adoptar medidas legislativas por las que se limite, en su totalidad o en parte, el derechos de acceso del interesado en la medida en que dicha limitación parcial o completa constituya una medida necesaria y proporcional en una sociedad democrática, teniendo debidamente en cuenta los intereses legítimos de la persona de que se trate:

a) para evitar que se obstaculicen pesquisas, investigaciones o procedimientos jurídicos u oficiales;

b) para evitar que se prejuzgue la prevención, detección, investigación y enjuiciamiento de infracciones penales o la ejecución de sanciones penales;

c) para proteger la seguridad pública;

d) para proteger la seguridad nacional;

[857] Artículo 13 de la propuesta de Directiva COM (2012) 10 final, de 25.1.2012.
[858] Artículo 21 de la propuesta de Reglamento General sobre Protección de Datos personales Dicho artículo «aclara la facultad otorgada a la Unión o a los Estados Miembros de mantener o introducir restricciones a los principios establecidos en el artículo 5 y a los derechos de los interesados establecidos en los artículos 11 a 20 y en el artículo 32. Esta disposición se basa en el artículo 13 de la Directiva 95/46/CE y en las obligaciones que emanan de la Carta de los Derechos Fundamentales y el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales, interpretados por el Tribunal de Justicia de la Unión Europea y el Tribunal Europeo de Derechos Humanos». Cfr. 4.3.5. Sección 5 – Restricciones, COM (2012) 11 final, de 25.1.2012.
[859] Considerando 82 de la propuesta de Directiva COM (2012) 10 final.

e) para proteger los derechos y libertades de otras personas.

2. Los Estados Miembros podrán determinar por ley las categorías de tratamiento de datos que pueden acogerse en todo o en parte a las exenciones del apartado 1.

3. En los casos contemplados en los apartados 1 y 2, los Estados Miembros dispondrán que el responsable del tratamiento informará por escrito al interesado sobre cualquier denegación o limitación de acceso, sobre las razones de la denegación y sobre las posibilidades de presentar a la autoridad de control una reclamación e interponer un recurso judicial. La información sobre los fundamentos de hecho o de Derecho en los que se sustenta la decisión podrá omitirse cuando el suministro de dicha información pueda comprometer uno de los fines contemplados en el apartado 1.

4. Los Estados Miembros velarán porque el responsable del tratamiento documente los motivos por los que no comunicó los fundamentos de hecho o de Derecho en los que se sustenta la decisión».

Lo anterior lo podríamos sintetizar en los siguientes términos. Las medidas legislativas que adopten los Estados Miembros para retrasar, limitar u omitir la información de los interesados o el acceso a sus datos personales, tienen como exigencia, para ser considerados una intromisión ilegítima: a) constituir una medida necesaria y proporcionada en una sociedad democrática; b) tener debidamente en cuenta los intereses legítimos del interesado; y c) que su finalidad no sea no perjudicar la prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales; ni tampoco la afección de la seguridad pública, la seguridad nacional, al interesado o los derechos y libertades de otras personas.[860] Como ya lo planteamos en el estudio del artículo 8 del CEDH, estos requisitos constituyen el denominado «test democrático de restricción de derechos».[861]

[860] Considerando 33 de la propuesta de Directiva COM (2012) 10 final.
[861] Al respecto véase aparado 1 del capítulo cuarto de este trabajo.

Al respecto, cabe recordar que el Convenio 108 de 1981, al regular las excepciones y litaciones al derecho a la protección de datos en su artículo 9, también exige que éstas «constituyan una medida necesaria en una sociedad democrática».[862] En la misma línea, el Tribunal Europeo de Derechos Humanos, al referirse a la garantía de la intimidad individual y familiar del art. 8 CEDH, aplicable también al tráfico de datos de carácter personal, ha reconocido que pudiera tener límites como la seguridad del Estado[863], o la persecución de infracciones penales[864], y también ha exigido que tales limitaciones estén previstas legalmente y sean las indispensables en una sociedad democrática. Estos implica que la ley que establezca esos límites sea accesible al individuo concernido por ella, que resulten previsibles las consecuencias que para él pueda tener su aplicación, y que los límites respondan a una necesidad social imperiosa, y sean adecuados y proporcionados para el logro de su propósito.[865]

Cabe tener presente aquí que tanto las acciones como las omisiones pueden constituir una injerencia en el derecho. En esta línea, el TEDH en su jurisprudencia, ha considerado injerencias al derecho a la protección de datos personales las medidas de vigilancia secreta, los registros personales, la toma de fotos, la grabación de cintas de audio, la toma de huellas dactilares o muestras de sangre, la vigilancia del domicilio, el embargo o incautación de documentos escritos y las escuchas telefónicas.[866] Esas injerencias pueden tener lugar en cualquier momento del tratamiento de los datos personales, por ejemplo, en el proceso de recogida, almacenamiento, o utilización de los datos personales.[867] El TEDH considera que se produce una injerencia cuando se recogen datos sin informar al titular de los mismos y sin su consentimiento. Este tipo de injerencias se produce con mayor frecuencia en los casos de investigaciones secretas en los que se utilizan aparatos de escuchas telefónicas o se graban imágenes con cámaras ocultas.[868]

---

[862] Artículo 9.2 del Convenio 108 de 1981, del Consejo de Europa.
[863] STEDH caso *Leander*, de 26 de marzo de 1987, § 47 y ss.
[864] SSTEDH, casos *Z*, de 25 de febrero de 1997, y *Funke*, de 25 de febrero de 1993.
[865] SSTEDH, caso *X* e *Y*, de 26 de marzo de 1985; caso *Leander*, de 26 de marzo de 1987; caso *Gaskin*, de 7 de julio de 1989; *mutatis mutandis*, caso *Funke*, de 25 de febrero de 1993; caso *Z*, de 25 de febrero de 1997.
[866] SSTEDH de 6 de septiembre de 1978, caso *Klass*; de 2 de agosto de 1984, caso *Malone*; de 24 de abril de 1990, caso *Kruslin*; de 25 de marzo de 1998, caso *Kopp*; y de 16 de febrero de 2000, caso *Amann*.
[867] STEDH de 4 de mayo de 2000, caso *Rotaru*.
[868] Los casos Klass, Malone, Huvig y Kruslin son los que definen de una manera muy precisa la

CAPITULO OCTAVO

TRANSFERENCIA DE DATOS PERSONALES A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES

SUMARIO: INTRODUCCIÓN. 1. CONDICIONES ESPECÍFICAS PARA LA TRANSFERENCIA INTERNACIONAL DE DATOS EN MATERIA DE PREVENCIÓN Y REPRESIÓN PENAL EN LA DECISIÓN MARCO 2008/977/JAI. 1.1. Finalidad. 1.2. Competencia. 1.3. Consentimiento. 1.4. Nivel de protección adecuado. 2. MODIFICACIONES QUE INTRODUCE LA PROPUESTA DE DIRECTIVA COM (2012) 10 FINAL. 2.1. Los nuevos elementos a evaluar por la Comisión para declarar el nivel de protección adecuado. *2.1.1. Estado de Derecho y acceso a la justicia. 2.1.2. Existencia y funcionamiento de autoridades de control. 2.1.3. Compromisos internacionales asumidos.* 2.2. Transferencia internacional de datos con fines de prevención y sanción penal mediante "garantías apropiadas". 2.3. Transferencia internacional de datos con fines de prevención o sanción penal realizadas bajo situaciones de "excepción justificadas". 2.4. Mecanismos de Cooperación Internacional entre la Comisión y las Autoridades de Control de Terceros Estados, como vía de solución de conflictos. 3. ANÁLISIS DE UN CASO CRÍTICO: LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES CONTENIDOS EN EL REGISTRO DE NOMBRES DE PASAJEROS (*PASSENGER NAME RECORD,* PNR) CON FINES DE PREVENCIÓN Y REPRESIÓN PENAL. 3.1. Contextualización del problema. 3.2.- Los registros de nombre de pasajeros (PNR). *3.2.1. ¿Qué es el PNR? 3.2.2. Fines y naturaleza de los datos incluidos en el PNR.* 3.3. Los acuerdos internacionales suscritos por la UE sobre transferencias de datos PNR. *3.3.1. Contexto de los acuerdos. 3.3.2. Acuerdo UE-EE.UU sobre PNR de 2004, bajo la Directiva 95/46/CE. 3.3.3. La Sentencia del Tribunal Europeo de Justicia que anula los Acuerdos. 3.3.4. El Acuerdo provisional de 2006. 3.3.5. El Acuerdo definitivo de 2007 entre la UE y Estados Unidos sobre transferencia de datos del PNR. 3.3.6. El Acuerdo de 2005 sobre la transferencia de los datos API/PNR entre la Unión Europea y Canadá. 3.3.7. El Acuerdo de 2008 sobre el PNR entre la Unión Europea y Australia.* 3.4. Análisis de la propuesta de 2007 para la creación de un PNR europeo.

INTRODUCCIÓN

La regulación internacional de la protección de datos personales está lejos de ser uniforme en los diversos sistemas jurídicos del mundo. De hecho, aún existen muchos Estados e, incluso, zonas geográficas sin regulación sobre la materia. En el mejor de los

casos los hay con una normativa general o específica, pero con deficiencias tales que no garantizan una adecuada protección de las personas cuyos datos están siendo tratados. Es por este motivo, junto a la utilización intensiva por parte de las autoridades públicas encargadas de la prevención y sanción penal, que la regulación de las transferencias internacionales de datos cobra cada día mayor importancia[869]

Ahora bien, si nos circunscribimos sólo a los Estados Miembros Unión Europea, podemos constatar que existen una serie de problemas comunes en materia de seguridad pública que no pueden ser solucionados sólo por medio de las legislaciones nacionales o acuerdo de cooperación limitados sólo a algunos Estados. Existe, por tanto, la necesidad de establecer un marco armonizado y coherente en el ámbito de la cooperación policial y judicial, que permita una adecuada transferencia de datos personales a través de las fronteras interiores de la UE, y que establezca las condiciones para las transferencias a terceros países, al tiempo que se garantice una protección efectiva de los derechos de las personas.

La finalidad general de la normativa comunitaria en materia de protección de datos, es garantizar al individuo el poder de control y disposición de sus propios datos, aun cuando éstos hayan salido de la jurisdicción del Estado al cual pertenece el ciudadano comunitario. Con ello, se garantiza a los titulares de los datos ciertos derechos ineluctables para el caso que se pretenda la transferencia de datos a países que no cuentan con una legislación sobre la materia, o donde esta no alcanza un nivel mínimo de garantías para sus titulares. Con este límite legal se pretende evitar lo que se ha denominado paraísos de datos o *data heavens*.[870] Así mismo, si no hubiera un límite legal para la transferencia internacional de datos personales, la protección de los titulares de los datos podría ser vulnerada a través de la deslocalización del tratamiento en un país donde el nivel de protección no exista o no sea adecuado. En efecto, es muy

[869] Sobre la regulación internacional de la protección de datos, véase *supra* Capítulo tercero de este trabajo.

[870] Algunos autores llegan a plantear que estos comportamientos integrarían una forma de defraudación internacional surgida de las propias necesidades de las sociedades modernas y democráticas, que vendría a sumarse a las ya clásicas formas de *dumping* social o ecológico, sería una suerte de *data dumping*. Al respecto, véase Diana SANCHO VILLA, *Transferencia internacional de datos personales.* Civitas, Pamplona, 2003, p. 30.

probable que si no existieran dichos límites, no se tomarían las precauciones necesarias para evitar el menoscabo de los derechos que buscaba proteger la legislación.[871]

En lo que respecta al marco regulatorio de la transferencia internacional de datos personales, está dado por normas de carácter obligatorias y otras de carácter facultativo u orientativo. Dentro de éstas últimas encontramos las Recomendaciones de las Naciones Unidas[872], de la OCDE[873] y de la APEC.[874] Por su parte, el Convenio n° 108 de 1981 del Consejo de Europa, considerado el primer acuerdo internacional de carácter vinculante sobre la materia, sólo regula el movimiento de datos entre países que lo hayan suscrito[875], por lo que fue necesario, en el año 2001, dictar un Protocolo Adicional que se ocupara de dos temas preteridos por el Convenio: las autoridades de control y las transferencia internacional de datos a terceros países.[876] Además, con la finalidad de ayudar a implementar los principios generales del Convenio, se dictaron varias Recomendaciones en diversos ámbitos específicos, entre ellas la Recomendación n° (87) 15 destinada a dar pautas sobre el tratamiento de datos personales por parte de la policía.[877]

Ahora bien, en el ámbito específico de la Unión Europea, el primer instrumento que reguló el tema fue la Directiva 95/46/CE.[878] No obstante, su ámbito de aplicación excluye expresamente a las materias propias del antiguo tercer pilar comunitario, esto es, la cooperación policial y judicial.[879] Al no existir un instrumento equivalente a la

[871] En el mismo sentido, véase Rosa BARCELÓ y María Verónica PÉREZ ASINARI, «Transferencia internacional de datos personales», en *Protección de Datos: Comentarios a la LOPD y su Reglamento de Desarrollo*, Tirant lo blanch, Valencia, 2009, pp. 141-142.
[872] Al respecto véase *supra* apartado 2, del Capítulo tercero de esta tesis.
[873] Al respecto véase *supra* apartado 1, del Capítulo tercero de esta tesis.
[874] Al respecto véase *supra* apartado 3, del Capítulo tercero de esta tesis.
[875] El artículo 12 se dedica a regular los *Flujos transfronterizos de datos de carácter personal y el derecho interno.*
[876] Al respecto véase *supra* apartado 1.2 del Capítulo cuarto.
[877] Al respecto véase *supra* apartado 1.3 del Capítulo cuarto.
[878] El Capítulo IV, lo dedica a regular las *Transferencia de Datos Personales a Países Terceros,* artículos 25 y 26 de la Directiva 95/46/CE. En España, La Ley 15/1999, Orgánica de Protección de Datos de Carácter Personal (LOPD) regula el tema de las transferencia internacional de datos en dos artículos: 33 y 34, bajo el epígrafe de "Movimiento internacional de datos", denominación que ya se encontraba en la derogada Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD).
[879] El ámbito de aplicación de la Directiva es el Espacio Económico Europeo. El artículo 3.2 de la Directiva, señala expresamente que «las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la

Directiva en el tercer pilar comunitario, toda la normativa que se dictó en éste ámbito específico tuvo que desarrollar normas particulares sobre protección de datos.[880] Esta situación sólo cambia parcialmente con la entrada en vigencia de la Decisión Marco 2008/977/JAI 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.[881]

1. CONDICIONES ESPECÍFICAS PARA LA TRANSFERENCIA INTERNACIONAL DE DATOS EN MATERIA DE PREVENCIÓN Y REPRESIÓN PENAL EN LA DECISIÓN MARCO 2008/977/JAI

La Decisión Marco 2008/977/JAI, actualmente vigente, contiene sólo una disposición (artículo 13) sobre transferencia internacional de datos a terceros Estados u organismos internacionales.[882] Antes de entrar al análisis de los requisitos o condiciones a cumplir para autorizar una transferencia internacional, queremos detenernos en otro punto. Llama la atención que el artículo 13 de la Decisión Marco esté redactado pensando en que otro Estado miembro de la Unión, que ha recibido los datos, pueda transferirlo a un tercer Estado u organismo internacional, es decir, se parte de la base de la existencia de una cesión o puesta a disposición previa de los datos entre Estados Miembros de la Unión, autorizando al Estado receptor de los datos a transferirlos a un tercer Estado u organismo internacional.

Dado que no hay otra disposición en la Decisión Marco destinada a regular las transferencias internacionales de datos, la norma tiene una falencia importante, ya que

---

seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal».

[880] Europol, Eurjust, VIS, SIS, etc.

[881] Publicado en el DOUE n° L 350 de 30.12.2008. Al respecto véase *supra* apartado 2.4 del Capítulo cuarto de esta tesis.

[882] Artículo 13 de la Decisión Marco 2008/977/JAI, cuyo epígrafe se titula *Transferencia a autoridades competentes de terceros Estados y a organismos internacionales*. La propuesta de Directiva COM(2012) 10 final, de 25.1.1012, que pretende derogar y reemplazar a la Decisión Marco citada, tiene un mayor desarrollo sobre la materia. En efecto, la propuesta dedica 6 artículo al tema, donde se regula, respectivamente: los *principios generales de las transferencias de datos personales* (artículo 33); *transferencias con una decisión de adecuación* (artículo 34); *transferencias mediante garantías apropiadas* (artículo 35); *excepciones* (artículo 36); *condiciones específicas para la transferencia de datos personales* (artículo 37) y la *cooperación internacional en el ámbito de la protección de datos personales* (artículo 38).

no regula la transferencia directa de un Estado miembro a un tercer Estado.[883] Por tanto, a falta de regulación en la Decisión Marco, dicha materia debería quedar supeditada a lo dispuesto en la legislación nacional de cada Estado miembro. No obstante, esta postura, tiene un doble potencial problema. Por una parte, puede ocurrir que el Estado miembro de la Unión no tenga regulada específicamente la transferencia internacional de datos personales con fines de prevención o represión penal y, por otro lado, ello podría provocar diferencias importantes entre los diversos régimen jurídicos de los Estados Miembros, en cuanto a los requisitos y condiciones para autorizar una transferencia internacional de datos con fines de prevención y represión penal.

Como forma de solventar el problema, podríamos aplicar la normativa genérica sobre protección de datos, que por regla general autoriza la transferencia internacional de dichos datos cuando sea con fines de seguridad pública o seguridad nacional. Solucionado el problema de la habilitación legal, el problema ahora es otro: bajo qué requisitos o condiciones debe permitirse dicha transferencia internacional. Creemos que si un Estado no ha establecido una regulación en la materia de forma específica, debería utilizarse como estándar mínimo y a todo evento, los requisitos copulativos consignados en la Decisión Marco para autorizar la transferencia internacional, que pasamos a revisar a continuación.

1.1. Finalidad

El primer requisito que debe cumplirse para autorizar la transferencia internacional de los datos es que la finalidad perseguida por dicha transferencia sea la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o para la ejecución de sanciones penales.[884] Este requisito también se contempla en la propuesta de Directiva COM (2012) 10 final, que pretende sustituir a la Decisión Marco

[883] Esta situación cambiaría de aprobarse la propuesta de Directiva COM (2012) 10 final, ya que ésta regula el tema partiendo del supuesto de que las autoridades competentes de un Estado miembro puedan realizar la respectiva transferencia internacional. En éste sentido, el artículo 33 dispone: «Los Estados Miembros dispondrán que cualquier transferencia de datos personales por las autoridades competentes que sean o vayan a ser objeto de tratamiento tras su transferencia a un tercer país o a una organización internacional, incluidas las transferencias ulteriores a otro tercer país u otra organización internacional, solo podrá realizarse si…»

[884] Artículo 13.1.a) de la Decisión Marco 2008/977/JAI.

2008/977/JAI.[885] Con ello se pone de manifiesto uno de los principios generales que rige el tratamiento de datos personales: el principio de finalidad, esto es, que el tratamiento de datos de carácter personal deba limitarse al cumplimiento de las finalidades determinadas, explícitas y legítimas de la persona responsable.[886] Bajo este principio, la persona responsable debe abstenerse de llevar a cabo tratamientos no compatibles con las finalidades para las que hubiese recabado los datos de carácter personal, a menos que cuente con el consentimiento inequívoco del interesado.[887]

1.2. Competencia

El segundo requisito o condición que debe cumplirse para permitir la transferencia internacional de datos es que la autoridad receptora del tercer Estado, o el organismo internacional receptor, sea competente para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales.[888] De acuerdo con la propia Decisión Marco, se entiende por autoridad competente «los servicios u organismos creados en virtud de actos jurídicos adoptados por el Consejo al amparo del título VI del Tratado de la Unión Europea, así como las autoridades policiales, judiciales, aduaneras y otras autoridades competentes de los Estados Miembros autorizadas por el Derecho nacional a tratar datos personales en el ámbito de la presente Decisión Marco».[889] Dichas autoridades deben actuar dentro del ámbito de las funciones y atribuciones, y están habilitadas, tanto para el envío como para la recepción de los datos. Pensamos que en el caso de las autoridades receptoras, el cumplimiento de este requisito se tendría que verificar por medio de la comprobación «formal» de que efectivamente, de acuerdo al derecho interno del Estado respectivo o la norma internacional correspondiente, dicha autoridad es competente en materia policial, aduanera, judicial o en otros ámbitos vinculados a la prevención, la investigación, la

[885] Artículo 33.a y Considerando 45 de la propuesta de Directiva COM (2012) 10 final.
[886] Considerando 21 de la propuesta de Directiva COM (2012) 10 final.
[887] Principio n° 9 de la *Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal*, 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada el 5 de noviembre de 2009 en Madrid.
[888] Artículo 13.1.b) de la Decisión Marco 2008/977/JAI.
[889] Artículo 2. letra h) de la Decisión Marco 2008/977/JAI.

detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales.[890]

1.3. Consentimiento

El tercer requisito es que el Estado miembro que proporcionó los datos haya consentido la transferencia de acuerdo con su Derecho nacional.[891] Por tanto, cuando los datos personales se transfieren de un Estado miembro a terceros países o a organismos internacionales, tal transferencia, en principio, únicamente debe efectuarse una vez que el Estado miembro del que se hayan obtenido los datos, haya dado su consentimiento a la transferencia.

Un punto importante, entonces, será la forma de manifestar dicho consentimiento. Al parecer, al legislador comunitario lo que interesa es facilitar de todas las formas posibles que se realicen las transferencias internacionales, es por ello que se permite que cada Estado miembro pueda determinar las modalidades de dicho consentimiento, incluso, por ejemplo, mediante un consentimiento general para categorías de información.[892]

Una manifestación clara de la voluntad del legislador europeo de favorecer la cooperación policial eficiente, es la posibilidad de **excepcionar** la transferencia internacional del requisito del consentimiento previo del Estado de origen de los datos, en caso de una «amenaza inmediata y grave a la seguridad pública de un Estado miembro o de un tercer Estado o a intereses esenciales de un Estado miembro».[893] La naturaleza de la amenaza a la seguridad pública de un Estado miembro o de un tercer Estado, debe ser lo bastante inmediata como para imposibilitar la obtención a tiempo del consentimiento previo.[894] Como se puede apreciar, queda a *discreción* del Estado transmitente la calificación de la gravedad e inmediatez de la amenaza, lo que puede llevar a abusos en caso de establecerse este medio como regla general para este tipo de

[890] Considerando 22 de la Decisión Marco 2008/977/JAI. La propuesta de Directiva COM (2012) 10 final, también contempla en su artículo 33.b, como requisito general que la autoridad receptora sea competente en materias de prevención o represión penal, para autorizar la transferencia internacional.
[891] Artículo 13.1.c) de la Decisión Marco 2008/977/JAI.
[892] Considerando 24 de la Decisión Marco 2008/977/JAI.
[893] Artículo 13.2 de la Decisión Marco 2008/977/JAI.
[894] Considerando 25 de la Decisión Marco 2008/977/JAI.

transferencias, por lo que creemos debe ser una facultad que se utilice de modo excepcional. De todas formas, existe la posibilidad de un control *a posteriori*, ya que las transferencias de esta naturaleza deben ser informadas sin demoras a la autoridad del Estado de origen de los datos encargada de otorgar su consentimiento.[895]

La amenaza a la seguridad pública no es la única causal habilitante señalada en la Decisión Marco para autorizar la transferencia sin consentimiento previo. También se podrían excepcionar de dicho consentimiento previo situaciones en que estén en juego otros intereses esenciales de igual importancia de un Estado miembro, como por ejemplo, cuando exista una amenaza inmediata y grave a las infraestructuras vitales de un Estado miembro o cuando el sistema financiero de este pueda quedar gravemente perturbado.[896]

1.4. Nivel de protección adecuado

El cuarto y último requisito señalado por la Decisión Marco 2008/977/JAI para autorizar una transferencia internacional de datos, es que el tercer Estado u organismo internacional de que se trate garantice un nivel adecuado de protección en el tratamiento de datos previsto.[897] Por tanto, cuando los datos personales se transfieren de un Estado miembro a terceros Estados o a organismos internacionales, éstos deben, en principio, gozar de un nivel de protección adecuado.[898]

---

[895] Artículo 13.2 de la Decisión Marco 2008/977/JAI.
[896] Considerando 25 de la Decisión Marco 2008/977/JAI.
[897] Artículo 13.1.d) de la Decisión Marco 2008/977/JAI.
[898] Considerando 23 de la Decisión Marco 2008/977/JAI. El tema relativo a qué debe entenderse por "protección adecuada", ha sido abordado por el Grupo de Trabajo del Artículo 29. Tomando la Directiva 95/46/CE como punto de partida, y teniendo en cuenta las disposiciones de otros textos internacionales sobre la protección de datos, el GT29 ha señalado que debería ser posible lograr un "núcleo" de principios de contenido de protección de datos y de requisitos de procedimiento o de aplicación, cuyo cumplimiento pudiera considerarse un requisito mínimo para juzgar adecuada la protección. Esta lista mínima no debería ser inamovible. En algunos casos será necesario ampliar la lista, mientras que en otros incluso sea posible reducirla. El grado de riesgo que la transferencia supone para el interesado será un factor importante para determinar los requisitos concretos de un caso determinado. A pesar de esta condición, la compilación de una lista básica de condiciones mínimas es un punto de partida útil para cualquier análisis, sobre todo en el ámbito específico de las transferencias de datos con fines de prevención y sanción penal. Cfr. Grupo de Trabajo sobre la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales. Documento de Trabajo *Transferencias de Datos Personales a Terceros Países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE*, aprobado por el GT29 el 24.7.1998.

Para evaluar que un tercer Estado o un organismo internacional tengan un nivel de protección adecuado se toman en consideración todas las circunstancias que concurran en una operación de transferencia de datos, o en un conjunto de operaciones de transferencia de datos. No obstante lo anterior, la Decisión Marco 2008/977/JAI toma en especial consideración algunos aspectos. Éstos son: la naturaleza de los datos; la finalidad y la duración de la operación u operaciones de tratamiento previstas; el Estado de origen y el Estado u organismo internacional de destino final de los datos; la normativa, tanto general como sectorial, vigente en el tercer Estado u organismo internacional de que se trate; y las normas profesionales y medidas de seguridad que sean de aplicación.[899]

La propuesta de Directiva COM (2012) 10 final, que pretende reemplazar y derogar la Decisión Marco 2008/977/JAI, innova sobre transferencia internacional de datos, estableciendo una serie de modificaciones respecto de la sistemática del articulado, así como respecto de los requisitos y condiciones bajo las cuales se pueden llevar a cabo dichas transferencias internacionales de datos con fines de prevención y sanción penal.

De partida, la propuesta de Directiva establece como principio general que «Los Estados Miembros dispondrán que cualquier transferencia de datos personales por las autoridades competentes que sean o vayan a ser objeto de tratamiento tras su transferencia a un tercer país o a una organización internacional, incluidas las transferencias ulteriores a otro tercer país u otra organización internacional, solo podrá realizarse si: a) la transferencia es necesaria para la prevención, investigación, detección o enjuiciamiento de infracciones penales o para la ejecución de sanciones penales; y b) el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo».[900]

Como se puede apreciar, la letra a) mantiene el requisito de finalidad consignado también en la Decisión Marco: que las transferencias a terceros países sólo podrán

[899] Artículo 13.4. de la Decisión Marco 2008/977/JAI. Este artículo es prácticamente idéntico a lo dispuesto a en el artículo 25.2 de la Directiva 95/46/CE.
[900] Artículo 33 de la propuesta de Directiva COM (2012) 10 final.

llevarse a cabo si son necesarias para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales.

El otro requisito es que el responsable y el encargado del tratamiento cumplan con las condiciones establecidas para la transferencia internacional de datos, tiene particular importancia en caso que el tratamiento este sujeto algún tipo de restricción en el Estado u organización de origen, ya que se le impone al responsable del tratamiento la obligación de informar al destinatario de toda restricción al tratamiento y de tomar todas las medidas razonables para garantizar que los destinatarios de los datos personales en el tercer país u organización internacional cumplan con estas restricciones.[901]

En los siguientes apartados de este capítulo, se analizarán las modificaciones que introduce la propuesta de Directiva respecto de la Decisión Marco vigente, en cuanto a los requisitos y condiciones para transferir datos a países que hayan sido declarados con un **nivel de protección adecuado** por parte de la Comisión.

2. MODIFICACIONES QUE INTRODUCE LA PROPUESTA DE DIRECTIVA COM(2012) 10 FINAL

La propuesta de Directiva sobre protección de datos con fines de prevención y sanción penal, contempla múltiples opciones para transferir datos desde un Estado de la Unión a un tercer Estado u organismo internacional, lo que a nuestro juicio deja claro nuevamente que se quiere privilegiar la cooperación policial efectiva en este tipo de tratamiento. En efecto, junto con la posibilidad de que la Comisión pueda declarar en forma general o específica para el ámbito de la cooperación policial, que un tercer país u organismo internacional posee un nivel de protección adecuado, existe la opción de transferir dichos datos a un tercer países que no garantice dicho nivel de protección adecuado, si es que se ha suscrito un acuerdo internacional entre las partes, o si se ofrece garantías suficientes para el tratamiento concreto de que se trate o, por último, la transferencia caiga dentro de algunas de las genéricas excepciones a la exigencia de un nivel de protección adecuado que se contemplan en la nueva propuesta.

[901] Artículo 37 de la propuesta de Directiva COM (2012) 10 final.

2.1. Elementos a evaluar por la Comisión sobre el nivel de protección

La primera de estas múltiples opciones mencionadas en la propuesta de Directiva para transferir datos a un tercer país o a una organización internacional con fines de prevención o sanción penal, es que la Comisión decidida que un tercer país o una organización internacional garanticen un nivel de protección adecuado.[902] La novedad de la propuesta de Directiva sobre éste punto, es que permite a la Comisión declarar con nivel de protección adecuado no sólo a los países u organizaciones internacional, sino también a un territorio o un sector de tratamiento en ese tercer país.[903]

La Decisión de adecuación del tercer país que adopte la Comisión, puede ser *genérica*, y en tal caso se sigue lo dispuesto en el futuro Reglamento General de Protección de Datos de la Unión Europea[904], o *específica* para el ámbito de la cooperación policial y la cooperación judicial en materia penal, mediante el procedimiento regulado en la propuesta de Directiva.[905] En este último caso, la Comisión podrá decidir, dentro del ámbito de aplicación de la Directiva, que un tercer país, o un territorio o un sector de tratamiento de datos en ese tercer país, así como una organización internacional, garantizan un nivel de protección adecuado.[906]

Cuando no exista una decisión de adecuación previa, la propuesta de Directiva COM (2012) 10 final, al igual que la Decisión Marco 2008/977/JAI, establece las condiciones o requisitos necesario para que la Comisión adopte una.[907] En tales casos, la Comisión evaluará la adecuación del nivel de protección, tomando en consideración los siguientes elementos:

---

[902] Al respecto, véase el artículo 25 de la Directiva 95/46/CE que rige para todos los ámbitos comprendidos en el antiguo primer pilar comunitario.
[903] Artículo 34.1. de la propuesta de Directiva COM (2012) 10 final.
[904] Artículo 38 y 41 de la propuesta de Reglamento general de protección de datos, COM (2012) 11 final, de 25.1.2012.
[905] Artículo 34.3 de la propuesta de Directiva COM (2012) 10 final. Los actos de ejecución, se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 57, apartado 2 de la propuesta.
[906] Ídem.
[907] Artículo 34.2 de la propuesta de Directiva COM (2012) 10 final.

2.1.1. Estado de Derecho y acceso a la justicia

El primer requisito a considerar por parte de la Comisión al momento de evaluar si un país, territorio, sector de tratamiento u organismos internacionales cumple con un nivel de protección adecuado, es verificar que «el Estado de Derecho, la legislación pertinente en vigor, tanto general como sectorial, en particular en lo que respecta a la seguridad pública, la defensa, la seguridad nacional, el Derecho penal, las medidas de seguridad en vigor en el país de que se trate o aplicables a la organización internacional en cuestión, así como los derechos efectivos y exigibles, incluido el derecho de recurso administrativo y judicial efectivo de los interesados, en particular de los residentes en la Unión cuyos datos personales estén siendo transferidos».[908] Como se puede apreciar, se toma como parámetro los valores fundamentales en los que se basa la Unión, en particular la protección de los Derechos Humanos. Es por ello que la Comisión debe tener en cuenta en qué medida en dicho tercer país se respeta el Estado de Derecho, el acceso a la justicia, así como las normas y principios internacionales relativos a los Derechos Humanos.[909]

2.1.2. Existencia y funcionamiento de autoridades de control

El segundo requisito a considerar por la Comisión al momento de evaluar el nivel de protección del país, territorio, sector u organismo internacional destinatario de los datos personales, para una transferencia con fines de cooperación policial, es «la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país u organización internacional de que se trate, encargadas de garantizar el cumplimiento de las normas en materia de protección de datos, de asistir y asesorar a los interesados en el ejercicio de sus derechos y de cooperar con las autoridades de control de la Unión y de los Estados Miembros».[910]

2.1.3. Compromisos internacionales asumidos

[908] Artículo 34.2. a) de la propuesta de Directiva COM (2012) 10 final.
[909] Considerando 47 de la propuesta de Directiva COM (2012) 10 final.
[910] Artículo 34.2. b) de la propuesta de Directiva COM (2012) 10 final.

Un tercer elemento a tener en consideración por parte de la Comisión al momento de evaluar el nivel de protección ofrecidos por terceros estados u organismo internacionales son «los compromisos internacionales asumidos por el tercer país o la organización internacional de que se trate».[911] Como ya mencionamos, si tomamos como parámetro los valores fundamentales en los que se basa la Unión, la Comisión debe tener en cuenta en qué medida en dicho tercer país se respetan los Derechos Humanos.

Analizados todos estos requisitos descritos previamente, la Comisión decidirá, dentro del ámbito de aplicación de la Directiva (cooperación policial y judicial), si un tercer país, o un territorio, o un sector de tratamiento de datos en ese tercer país, o una organización internacional, garantizan o no un nivel de protección adecuado. En el caso que la Comisión decida que el lugar de destino al cual se pretende transferir los datos no garantiza un nivel de protección adecuado, se deben tomar las medidas y resguardos necesarios para las personas en lo que respecta a su derecho a la protección de datos personales, siguiendo para ello el procedimiento contemplado en la propia Directiva.[912] En estos casos los Estados Miembros deben cumplir la decisión de la Comisión, prohibiendo toda transferencia de datos personales al tercer país, o a un territorio, o un sector de tratamiento de datos en ese tercer país, o a la organización internacional de que se trate. De todas formas dicha decisión no es irreversible, ya que la propia Directiva faculta a la Comisión para entablar consultas con el tercer país o la organización internacional con vistas a poner remedio a esta prohibición de transferencia de datos.[913]

Para llevar un registro público de las decisiones de adecuación, la Comisión publicará en el Diario Oficial de la Unión Europea una lista de los terceros países, territorios y sectores de tratamiento de datos en un tercer país o una organización internacional, para los que haya decidido que está o no está garantizado un nivel protección adecuado.[914]

[911] Artículo 34.2. c) de la propuesta de Directiva COM (2012) 10 final.
[912] Artículo 57.2 y 3. de la propuesta de Directiva COM (2012) 10 final.
[913] Artículo 34.6 de la propuesta de Directiva COM (2012) 10 final.
[914] Artículo 34.7 de la propuesta de Directiva COM (2012) 10 final. La lista de terceros países que han sido declarados con nivel adecuado de protección se encuentra disponible en el sitio web de la Comisión: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm [Consultado en 27.1.2014]

2.2. Transferencia internacional de datos con fines de prevención y sanción penal mediante "garantías apropiadas"

Como señalamos anteriormente en este capítulo, la propuesta de Directiva COM (2012) 10 final, que pretende reemplazar y derogar la Decisión Marco 2008/977/JAI, es bastante "generosa" a la hora de establecer mecanismos que autoricen la transferencia internacional de datos. Así, en ausencia de una decisión de adecuación de la Comisión que declare si el lugar de destino de los datos posee un nivel de protección adecuado, se pueden efectuar igualmente transferencias internacionales de datos, siempre que el tercer país u organismo internacional ofrezca "garantías apropiadas".[915]

La propuesta no explicita en ninguna parte garantías respecto de qué se están solicitando, a diferencia de lo que ocurre, por ejemplo, con la Directiva 95/46/CE, que específicamente señala qué son «garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos».[916] Lo que sí señala la propuesta de Directiva es cómo se deben acreditar dichas garantías, que puede ser por dos vías. La primera, mediante un instrumento jurídicamente vinculante, como un acuerdo internacional[917]; y la segunda, como alternativa a la anterior, es que el responsable o el encargado del tratamiento evalúen todas las circunstancias que concurren en la transferencia de datos personales y lleguen a la conclusión de que existen garantías apropiadas con respecto a la protección de datos personales.[918]

Ésta última hipótesis, en que el responsable o el encargado del tratamiento puedan, sobre la base de una evaluación de las circunstancias que concurran en la transferencia, concluir que existen garantías suficientes, nos parece peligrosa. Si bien, dicha evaluación debe ser adoptada por personal debidamente autorizado (autoridad competentes en el ámbito policial o judicial) y ser debidamente documentada, no existe

[915] Artículo 35.1 de la propuesta de Directiva COM (2012) 10 final.
[916] Artículo 26.2 de la Directiva 95/46/CE.
[917] Artículo 35.1. a) de la propuesta de Directiva COM (2012) 10 final. Ejemplos de acuerdo internacionales sobre la materia, son los Acuerdos entre la Unión Europea y Estados Unidos sobre los Registros de Nombres de pasajeros (*Passenger Name Record*, PNR) y el Acuerdo de Puerto Seguro (*Safe Harbour*).
[918] Artículo 35.1. b) de la propuesta de Directiva COM (2012) 10 final.

un control *a priori* de la una autoridad de control, ya que sólo se permite la intervención de ésta *a posteriori*.[919] En éste punto la propuesta de Directiva se diferencia de la propuesta de Reglamento general de protección de datos, ya que ésta última, expresamente, exige que deba obtenerse una autorización de la autoridad de control antes de proceder a la transferencia internacional de los datos.[920] Además, creemos que esta forma de autorización de las transferencias internacionales de datos desincentivará a los países y organismos internacionales a solicitar a la Comisión ser evaluadas de acuerdo al parámetro del nivel de protección adecuado, que aplica estándares europeos en la materia.

2.3. Transferencia internacional de datos con fines de prevención o sanción penal realizadas bajo situaciones de "excepción justificadas"

Por últimos, existen un conjunto de situaciones que, inspiradas en el artículo 26 de la Directiva 95/46/CE y el artículo 13 de la Decisión Marco 2008/977/JAI, se encuentran eximidas del cumplimiento de cualquier requisito o condición para su transferencia internacional.[921] Estas son:

a) que la transferencia sea necesaria para proteger los **intereses vitales** del interesado o de otra persona.[922] Aunque no lo dice expresamente, a diferencia de la propuesta de Reglamento general de protección de datos, la protección de los intereses vitales del interesado se refiere al caso en que éste esté física o jurídicamente incapacitado para dar su consentimiento;[923]

b) la transferencia sea necesaria para salvaguardar **intereses legítimos** del interesado cuando así lo disponga el Derecho del Estado miembro que transfiere los datos personales;

c) la transferencia de los datos sea esencial para prevenir una amenaza inminente y grave para la **seguridad pública** de un Estado miembro o de un tercer país;

[919] Artículo 35.2 de la propuesta de Directiva COM (2012) 10 final.
[920] Artículo 42.4 y 5 de la propuesta de Reglamento general de protección de datos, COM (2012) 11 final.
[921] Artículo 36 de la propuesta de Directiva, COM (2012) 10 final.
[922] Artículo 36 a) de la propuesta de Directiva, COM (2012) 10 final.
[923] Artículo 44.1 f) de la propuesta de Reglamento general de protección de datos, COM (2012) 11 final.

d) la transferencia sea necesaria en casos concretos a efectos de **prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales**;

e) la transferencia sea necesaria en casos concretos para el **reconocimiento, el ejercicio o la defensa de un derecho en un procedimiento judicial** relativo a la prevención, investigación, detección o enjuiciamiento de una infracción penal o la ejecución de una sanción penal específica.

Las cinco causales de excepción mencionadas pueden ser reconducidas a dos categorías: las que miran al interés del titular de los datos o de un tercero, y las que miran por la protección de un interés público preponderante, cuyo caso está dado por la prevención o sanción penal. Dentro de ésta última categoría incluimos las que miran el interés legítimo del responsable o del encargado del tratamiento, que en cuyos casos, son por regla general, las autoridades encargadas de la prevención o sanción penal.

Por último, cabe destacar que en todos los casos señalados precedentemente como excepcionales, se *puede* autorizar la transferencia, aun cuando el lugar de destino no tenga un nivel adecuado de protección, o el país u organización respectiva no haya dado garantías suficientes de que se respetarán los derechos de los interesados.

3. MECANISMOS DE COOPERACIÓN INTERNACIONAL ENTRE LA COMISIÓN Y LAS AUTORIDADES DE CONTROL DE TERCEROS ESTADOS COMO VÍA DE SOLUCIÓN DE CONFLICTOS

Cuando los datos personales circulan a través de las fronteras se pone en mayor riesgo la capacidad de las personas físicas para ejercer sus derechos frente a la utilización ilícita de sus datos. Al mismo tiempo, es posible que las autoridades de control se vean en la imposibilidad de tramitar reclamaciones o realizar investigaciones relativas a actividades desarrolladas fuera de sus fronteras. Además, los esfuerzos por colaborar en el contexto transfronterizo también pueden verse obstaculizados por poderes preventivos o correctores insuficientes y regímenes jurídicos incoherentes. Por

tanto, es necesario fomentar una cooperación más estrecha entre las autoridades de control de protección de datos para ayudarles a intercambiar información con sus homólogos extranjeros.[924]

En ésta línea, la propuesta de Directiva establece explícitamente mecanismos de cooperación internacional para la protección de los datos personales entre la Comisión y las autoridades de control de terceros países, en particular aquellos que se considere que ofrecen un nivel de protección adecuado, teniendo en cuenta la Recomendación de la OCDE relativa a la cooperación transfronteriza en la aplicación de las legislaciones que protegen la privacidad, de 12 de junio de 2007.[925]

Entre las *medidas concretas* que se proponen se encuentran: a) crear mecanismos de cooperación internacional eficaces que faciliten la aplicación de la legislación relativa a la protección de datos personales; b) prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías apropiadas para la protección de los datos personales y otros derechos y libertades fundamentales; c) procurar la participación de las partes interesadas pertinentes en los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales; d) promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales.[926]

4. ANÁLISIS DE UN CASO CRÍTICO: LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES CONTENIDOS EN EL REGISTRO DE NOMBRES DE PASAJEROS *(PASENNGER NAME RECORD* - PNR) CON FINES DE PREVENCIÓN Y REPRESIÓN PENAL

[924] Considerando 50 de la propuesta de Directiva, COM (2012) 10 final.
[925] Artículo 38 de la propuesta de Directiva, COM (2012) 10 final.
[926] Artículo 38.1 de la propuesta de Directiva, COM (2012) 10 final.

4.1. Contextualización del problema

En la última década, y como consecuencia de los ataques terroristas ocurridos en Nueva York (2001), Madrid (2004) y Londres (2005), se han ido impulsando progresivamente una serie de medidas destinadas a combatir el terrorismo.[927] Algunas de estas medidas propugnan el tratamiento —recopilación, conservación, análisis y transferencia— de distintos tipos de datos de carácter personal, bajo el argumento que ello permitiría a las autoridades nacionales competentes combatir de manera efectiva al terrorismo y las formas graves de delincuencia.[928] Así, en el transcurso de los últimos años, Europa ha ido adoptando distintas iniciativas en esta línea, como la adopción de la Directiva que permite la conservación de datos sobre el tráfico de telecomunicaciones y de localización;[929] la Iniciativa sueca para simplificar el intercambio transfronterizo de información en investigaciones penales y operaciones de inteligencia;[930] y la Decisión que agiliza el intercambio de perfiles de ADN, impresiones dactilares y datos de los registros de matriculación de vehículos en la lucha contra el terrorismo y otras formas de delincuencia.[931] Una medida significativa, que incluye la recogida, tratamiento e intercambio de datos personales, es la utilización de los datos de los registros de nombres de los pasajeros (*Passenger Names Record*, PNR) con fines preventivos y represivos. Todas estas medidas constituyen un ejemplo de los programas impulsados,

[927] Para un estudio detallado sobre el terrorismo actual, véase Joan Lluís PÉREZ FRANCESCH, y Tomás Gil MÁRQUEZ, *El Terrorisme Global.* Ed. UOC, Barcelona, 2009; Isabel DELGADO LIROLA. Terrorismo y cooperación penal:¿un contexto más favorable para los derechos humanos en las relaciones transatlánticas?. En *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz 2009*. Universidad del País Vasco, 2010, pp. 363-394. Sobre las tensiones actuales entre los valores de la libertad y la seguridad, después del 11-S, desde diversas perspectivas, puede consultarse el libro colectivo, Joan Lluís PÉREZ FRANCESCH (coord), *Libertad, seguridad y transformaciones del Estado*, ICPS, Barcelona, 2009.

[928] A modo de ejemplo, véase la exposición de motivos de la Propuesta de Decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros (*Passenger Name Record* - PNR) con fines represivos. COM (2007) 654 final, de fecha 6.11.2007, pp. 2-3.

[929] Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. Publicada en el Diario Oficial de la UE nº L 105/54, con fecha 13.4.2006

[930] Decisión marco 2006/960/JAI del Consejo, de 18 de diciembre de 2006, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados Miembros de la Unión Europea. Publicada en el Diario Oficial de la UE n° L 386 de 29.12.2006

[931] Decisión 2008/616/JAI del Consejo, de 23 de junio de 2008, relativa a la ejecución de la Decisión 2008/615/JAI sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza. Publicada en el Diario Oficial de la UE nº L 210/12 de fecha 6.8.2008. Esta Decisión incorpora el Tratado de Prüm al ordenamiento jurídico europeo. Para un completo estudio sobre el Tratado de Prüm, véase el número monográfico dedicado al mismo en la *Revista de Derecho Constitucional Europeo* (ReDCE), Número 7, Enero-Junio de 2007, disponible en http://www.ugr.es/~redce/REDCE7pdf/ReDCE7.pdf

tanto por la Unión Europea y algunos de sus Estados Miembros como por terceros Estados, destinados a gestionar (recoger e intercambiar) la información y datos de personales en el marco de la lucha contra el terrorismo y la delincuencia grave de carácter transnacional.[932]

Es importante destacar que la lucha contra el terrorismo se debe dar con las armas que entrega el Estado democrático de Derecho. Lo anterior implica que las medidas que se adopten y la forma cómo se apliquen, deben conducir a fortalecer la sociedad democrática y el respeto a los derechos y libertades fundamentales. Lo contrario implicaría ponerse al mismo nivel de los que quieren violentar la sociedad mediante el miedo y el terror, y en el peor de los casos, podemos llegar a una sociedad del control, donde los derechos de los ciudadanos se vean constreñidos en pro de una real o aparente "sensación" de mayor seguridad.

Los Acuerdos suscritos por la Unión Europea con terceros países (EE.UU, Canadá, Australia) y el proyecto de Decisión Marco sobre tratamiento de datos personales contenidos en el registro de nombre de pasajeros (PNR), es una medida que afecta claramente derechos fundamentales, en particular la privacidad y los datos de carácter personal. Por tanto, éstas medidas deben someterse a los controles necesarios con objeto de verificar si las restricciones y limitaciones que se imponen a dichos derechos obedecen a criterios de racionalidad y proporcionalidad que, a nuestro juicio, deben guiar el combate al terrorismo.

4.2. Los registros de nombres de pasajeros (PNR)

4.2.1. ¿Qué es el PNR?

La denominación PNR *(Passenger Name Records)* es la sigla inglesa utilizada para referirse a los registros de nombres de los pasajeros. Estos registros contienen toda la información necesaria de cada viajero para la tramitación, reserva y el control de

[932] Al respecto, véase la Comunicación COM(2010)385 final, de la Comisión al Consejo y al Parlamento Europeo, sobre el "Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia", de fecha 20.7.2010

salidas por parte de las compañías aéreas. Con ellos se elabora una base de datos, que contiene diferentes categorías de información sobre una persona, tales como el nombre, apellido, número de pasaporte o documento nacional de identidad, número de teléfono, dirección; información de carácter financiero, como la forma de pago y el número de tarjeta con la que se realizó la reserva; los datos propios del viaje: fechas, itinerario, datos del billete, número de asiento, equipaje. Adicionalmente, algunos de los acuerdos exigen otro tipo de información calificada como "suplementaria", que incluye datos sobre billetes sólo de ida, situación de *stand by* y de "no presentados"; información sobre otros servicios (*Other Service Information*, en adelante "OSI"), información sobre servicios especiales solicitados (*Special Services Information,* en adelante "SSI") y sobre servicios especiales solicitados (*Special Services Reserved*, en adelante "SSR").[933] Por último, la información recopilada debe contener todo el historial de cambios de los datos de PNR y los datos recogidos en el sistema de información anticipada sobre los pasajeros (*Advance Passenger Information*, API).[934]

Las compañías aéreas, junto con la obligación de entregar los datos PNR de cada pasajero, deben también poner a disposición de las autoridades competentes en materia migratoria de cada Estado europeo los datos del sistema API, que igual que el PNR colecta los datos personales del pasajero por adelantado. Este sistema contiene, entre otros, información sobre "datos biográficos" del pasajero, como son el número y el tipo de documento de viaje utilizado, el nombre y apellidos, el lugar de residencia, el lugar y fecha de nacimiento y la nacionalidad de la persona. También contiene información sobre el paso fronterizo de entrada en el territorio de los Estados Miembros de la Unión Europea, el código de transporte, la hora de salida y de llegada del transporte, el número total de personas transportadas en ese medio y el lugar inicial de embarque. La regulación principal de esta materia se encuentra en la Directiva 2004/82/CE.[935] Su objeto es mejorar los controles fronterizos y combatir la inmigración ilegal mediante la comunicación anticipada de los datos de las personas transportadas por parte de los transportistas a las autoridades competentes en cada Estado europeo.

[933] Cfr. El Título III, de la Carta de los EE.UU. a la UE, anexa al Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (Acuerdo PNR 2007). Publicada en el Diario Oficial de la UE nº L 204 de 4.8.2007, p. 21

[934] Ídem.

[935] Directiva 2004/82/CE de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas. Publicada en el DOUE n° L 261 de 6.8.2004.

La principal diferencia entre los datos del PNR y los del API es su **finalidad**. Los datos del PNR se utilizan principalmente como un instrumento para la prevención y represión de ilícitos terroristas y formas graves de delitos transnacionales, en cambio, los datos API se utilizan esencialmente para el control de identidad en los pasos fronterizos europeos y en el combate a la inmigración ilegal. No obstante lo anterior, y como tendremos oportunidad de ver más adelante en este trabajo, algunos acuerdos suscritos por la Unión Europea y la propuesta de Decisión Marco que pretende la instauración de un PNR europeo, contemplan a los datos API como uno de los elementos a transferir dentro del PNR. Lo anterior se ha justificado señalando que «los datos API también puede ayudar a identificar a terroristas y delincuentes conocidos al contrastar si sus nombres aparecen en un sistema de alerta como el SIS».[936] Otra diferencia entre ambos tipos de datos es la **disponibilidad**, ya que de los datos del PNR se obtienen una mayor anticipación que los datos API. Por último, otra gran diferencia entre ambos tipos de datos es la **fiabilidad** de la información contenida en ellos, puesto que mientras los datos PNR son recogidos por la compañías aéreas en base a lo que informan los eventuales pasajeros, sin que exista certeza sobre su autenticidad, los datos API son recolectados desde documentos oficiales (Pasaportes, DNI, entre otros) que, en principio, dan una mayor seguridad sobre su legitimidad.

4.2.2. Fines y naturaleza de los datos incluidos en el PNR

En principio, la justificación para autorizar el tratamiento los datos de carácter personal contenidos en el PNR es la *prevención y represión del terrorismo*. No obstante, como tendremos oportunidad de ver más adelante, algunos de los Acuerdos suscritos por la Unión han ido añadiendo otros fines. Así por ejemplo, en el último Acuerdo suscrito entre la UE y Estados Unidos, se señala que dichos datos se utilizarán con la finalidad de prevenir y combatir el terrorismo, pero también se mencionan como fines habilitantes para el tratamiento a los delitos conexos al terrorismo y otros delitos graves, incluida la delincuencia organizada de naturaleza transnacional, y también incluye como fin habilitante las medidas contra la fuga en caso de orden de arresto o detención por los

[936] Cfr. Propuesta de Decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros (*Passenger Name Record* - PNR) con fines represivos, COM (2007) 654 final, de fecha 6.11.2007, p. 3

delitos antes señalados.[937] Esta peligrosa extensión de los fines que habilitan el tratamiento de los datos personales contenidos en el PNR ha sido duramente criticada tanto por el Supervisor Europeo de Protección de Datos, como por el Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE[938], críticas que analizaremos más adelante en profundidad.

A esta extensión de los fines que habilitan el uso de los datos del PNR se ha añadido el problema de su uso con fines **preventivos**. Es decir, se pretende la utilización de este tipo de datos para contrastar determinados indicadores de riesgo, con el fin de identificar a los sospechosos. Es claro que esta forma de uso de los datos PNR es sumamente peligrosa, ya que se utilizan para el análisis y la creación de modelos de comportamiento general, y particularmente, para el estudio de los comportamientos de viajes aéreos de todos los pasajeros. Ello da cabida a la realización de perfiles de sospechosos.[939] Lo anterior, estaría en abierta contradicción con las disposiciones europeas de protección de datos personales. Debemos considerar que casi todos los datos contenidos en el PNR pueden calificarse jurídicamente como datos de carácter personal, ya que permiten identificar a una persona o la hacen identificable, por tanto son aplicables a su respecto todas las disposiciones que regulan esta materia en Europa y sus Estados Miembros, las que en principio tienen prohibida la elaboración de perfiles de los interesados, salvo habilitación legal expresa.

Otro problema vinculado al uso de los datos contenidos en el PNR, es el **tiempo de retención** de los mismos. Al inicio de las primeras negociaciones entre la UE y Estados Unidos, éstos querían que dicho período fuera de cincuenta años, lo que a todas luces es excesivo. Actualmente, los acuerdos vigentes distinguen dos tipos de bases de datos para determinar el periodo de conservación: activas e inactivas. Así, por ejemplo, en el último acuerdo suscrito con los EE.UU., los datos del PNR originarios de la UE se

[937] Cfr. El punto nº 1 de la Carta de los EE.UU. a la UE, anexa al Acuerdo entre la Unión Europea y los Estados Unidos de América (Acuerdo PNR 2007).
[938] Este Grupo de Trabajo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Es un órgano de carácter consultivo independiente de la UE, que se pronuncia sobre los temas vinculados a la protección de los datos y la vida privada. Sus tareas se definen en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE.
[939] Cfr. El nº 1 de la Propuesta de Resolución del Parlamento Europeo, sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países y las Recomendaciones de la Comisión al Consejo para autorizar la apertura de negociaciones para un Acuerdo entre la Unión Europea y Australia, Canadá y los Estados Unidos. B7-0604/2010/rev.2, de fecha 3.11.2010, pp. 6-7

conservan siete años en una base de datos activa, y posteriormente pasan a una base de datos inactiva por un periodo de ocho años más. En el Acuerdo con Australia, el periodo de conservación en la base de datos activa es de tres años y medio, y posteriormente pasan a la base de datos inactiva durante dos años más. En Canadá, los datos se conservan durante tres años y medio, pasando la información al anonimato al cabo de setenta y dos horas. En la propuesta de Decisión Marco, el periodo de conservación es de cinco años en la base activa y ocho más en la inactiva. En todo caso, una vez que los datos se encuentran en las bases de datos inactivas, en principio, estos países sólo podrían acceder a dicha base en los supuestos expresamente contemplados en los acuerdos, y por autoridades expresamente facultadas para dicho efectos.[940] Una vez expirado todo el periodo (en bases activas e inactivas), las autoridades competentes deberían proceder a cancelar y borrar todos los datos contenidos en el PNR.

También ha sido materia de un intenso debate, el **método de la transferencia** de datos. Los acuerdos suscritos hasta ahora y la propuesta de Decisión Marco hacen referencia a dos sistemas. En primer lugar, el sistema *pull*, según el cual las autoridades que requieren los datos pueden acceder directamente al sistema de reservas de la compañía aérea y copiar los datos requeridos en su propia base de datos. En segundo lugar, el sistema de transmisión *push*, por el cual las propias compañías aéreas transmiten los datos PNR requeridos a la base de datos de la autoridad requirente, es decir, la compañía aérea transmite los datos al tercer país, sin permitir el acceso de estos a sus bases de datos. Este último sistema brinda un nivel de protección más alto a los datos de carácter personal, ya que permite un mayor control por parte de las autoridades europeas de protección de datos y reduce los riesgos de una posible invasión excesiva a la privacidad de los pasajeros.

[940] Al respecto véase COM (2010)385 final, de 20.7.2010.

4.3. Los Acuerdos internacionales suscritos por la UE sobre transferencias de datos PNR

4.3.1. Contexto de los acuerdos

Después de los ataques terroristas del 11 de septiembre de 2001, Estados Unidos de Norteamérica adoptó una serie de medidas, tanto de carácter preventivo como represivo, destinadas a combatir la amenaza terrorista.[941] En el intento de asegurar la eficacia de dichas medidas, el gobierno de EE.UU. consideró fundamental controlar y analizar los flujos de datos personales relativos a los pasajeros aéreos. Para ello, en noviembre de 2001, se aprobó una ley que obliga a cualquier compañía aérea que opere vuelos de pasajeros con destino u origen en los Estados Unidos, a proporcionar a la Oficina de Aduanas y Protección Fronteriza (*Bureau of Customs and Border Protection*; en lo sucesivo, el CBP) el acceso electrónico a los datos del PNR.[942]

En junio de 2002, la Comisión Europea, reconociendo los legítimos intereses de seguridad en juego, informó a las autoridades de los Estados Unidos que tales requisitos podrían entrar en conflicto con la legislación comunitaria y de los Estados Miembros relativa a la protección de datos, así como con determinadas disposiciones del Reglamento relativo a los Sistemas Informatizados de Reserva (SIR).[943] Los problemas de compatibilidad entre la legislación de EE.UU. y las normas comunitarias de protección de intimidad de las personas, fueron planteadas principalmente por el Grupo de Trabajo del artículo 29 sobre protección de datos, el Parlamento Europeo y la Comisión Europea.

---

[941] Para un estudio detallado sobre el tema, véase Michelle NINO, «The protection of personal data in the fight against terrorismo. New perspectives of PNR European Union instruments in the light of the Treaty of Lisbon», *Utrecht Law Review* / Volume 6, Issue 1 (January) 2010, pp. 62-85, disponible en http://www.utrechtlawreview.org

[942] Cfr. Aviation and Transportation Security Act (ATSA), 19 November 2001 (Public Law 107–71, 107th Congress, 49 USC Section 44909(c)(3) (2001)); y en 2002, the US passed legislation concerning border security (Enhanced Border Security and Visa Entry Reform Act of 2002 (EBSV), 5 May 2002).

[943] Reglamento (CEE) nº 2299/89 del Consejo, de 24 de julio de 1989, por el que se establece un código de conducta para los sistemas informatizados de reserva, Diario Oficial de la UE nº L 220 de 29.7.1989, p. 1, cuya última modificación la constituye el Reglamento (CE) nº 323/1999 del Consejo, de 8 de febrero de 1999, Diario Oficial de la UE nº L 40 de 13.2.1999, p. 1.

El GT29[944] recalcó la necesidad de alcanzar un equilibrio adecuado entre las necesidades de seguridad y la protección de las garantías individuales, teniendo en cuenta el derecho del individuo a la protección de datos personales como parte de los derechos y libertades fundamentales protegidos por la Unión Europea. Asimismo, declaró que el cumplimiento por parte de las compañías aéreas de la legislación de los EE.UU. probablemente causará problemas en relación con la Directiva 95/46/CE y expresó su preocupación en cuanto al nivel de protección de datos personales en dicho país.[945]

El Parlamento Europeo, por su parte, criticó las posiciones iniciales de la Comisión, invitándola a que las medidas por adoptar en el ámbito de la transferencia de datos PNR en los EE.UU., fueran respetuosas de la legislación comunitaria y del Convenio Europeo de Derechos Humanos. En particular, el Parlamento Europeo, expresó sus dudas sobre la eficacia real de la transferencia de los datos del PNR en la lucha contra el terrorismo internacional, subrayando que esta estrategia podría haber creado un sistema masivo de control, en completa violación de los principios previstos en la Directiva 95/46/CE, el artículo 8 del CEDH y los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea.[946]

La Comisión Europea, de acuerdo con el artículo 25 de la Directiva 95/46, está facultada para evaluar si la transferencia de datos personales a un tercer país garantiza un nivel adecuado de protección de dichos datos en virtud de la legislación comunitaria. Al realizar el examen de los antecedentes para pronunciar su declaración sobre el nivel de adecuación, la Comisión mostró su preocupación por la invasión de la legislación

[944] Dictamen 10/2001 de 14 de diciembre 2001, del Grupo de Trabajo del artículo 29, sobre la necesidad de un enfoque equilibrado en la lucha contra el terrorismo. Disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/2001/common/pdfs/Dictamen-10-2001.pdf [fecha consulta 5.1.2014]

[945] Cfr. Los Dictámenes 6/2002 del Grupo de Trabajo del artículo 29, relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a los Estados Unidos, de fecha 24.10.2002; y Dictamen 4/2003 relativo al nivel de protección garantizado en los EE.UU. para la transferencia de datos de pasajeros, de fecha 13.6.2003, ambos disponibles en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/common/B.2.62-cp--wp66---APIS.pdf [fecha consulta 5.1.2014].

[946] Cfr. Resolución del Parlamento Europeo sobre la transmisión de datos personales por las compañías aéreas en los vuelos transatlánticos, P5_TA(2003)0097, de fecha 13.3.2003. Publicado en Diario Oficial de la UE n° C 061 E de 10.03.2004 p. 381-384; y la Resolución del Parlamento Europeo sobre la transmisión de datos personales por las compañías aéreas en los vuelos transatlánticos: estado de las negociaciones con los EE.UU, P5_TA(2003)0429, de fecha 9.10.2003, publicada en el Diario Oficial de la UE nº C 81 E/105 de fecha 31.3.2004.

estadounidense y su capacidad potencial para limitar la privacidad de los individuos. Se informó a las autoridades de EE.UU. de que la ley que exigía a las compañías aéreas la entrega de los datos consignados en el PNR podría violar algunas normas comunitarias importantes en materia de protección de datos personales y los sistemas informatizados de reserva. Las autoridades estadounidenses aplazaron la entrada en vigor de los nuevos requisitos impuestos a las aerolíneas, pero finalmente se negaron a renunciar a la imposición de sanciones a las compañías que no los cumplían después del 5 de marzo de 2003, lo que provocó que muchas de las grandes compañías aéreas de la Unión Europea permitieran el acceso a sus PNR desde entonces.[947]

El 18 de febrero de 2003, la Comisión Europea y el Gobierno de Estados Unidos hicieron pública una declaración conjunta en la que recordaban su interés común en combatir el terrorismo.[948] Asimismo, con objeto de que la Comisión pudiera adoptar una Decisión con arreglo al artículo 25.6 de la Directiva 95/46/CE, relativa a la protección de datos, en la que se reconozca el carácter adecuado de la protección ofrecida a los datos transmitidos, la CBP suscribió unos compromisos *(undertakings)* en los que se obligaba a proporcionar una protección adecuada al tratamiento de los datos de los registros de nombres de pasajeros.[949]

Las negociaciones tuvieron por objeto acercar a las normas comunitarias la utilización y protección de los datos de los PNR por parte de Estados Unidos. En dos Resoluciones, de 13 de marzo de 2003 y de 9 de octubre de 2003, el Parlamento Europeo pidió a la Comisión que tomase una serie de medidas relativas a la transferencia de datos de PNR a Estados Unidos, con el fin de garantizar que se tuviesen en cuenta las preocupaciones europeas respecto a la protección de datos.[950]

---

[947] Cfr. Comunicación de la Comisión al Consejo y al Parlamento Europeo - Transferencia de datos de los registros de nombres de los pasajeros (PNR): un enfoque global de la Unión Europea, COM (2003) 826 final, de fecha 16.12.2003.

[948] *Idem.*

[949] Estos "Compromisos" *(undertakings)* fueron suscritos por la Oficina de Aduanas y Protección Fronteriza del Departamento de Seguridad Nacional (CBP) con fecha 11.5.2004.

[950] Resolución del Parlamento Europeo sobre la transmisión de datos personales por las compañías aéreas en los vuelos transatlánticos, P5_TA(2003)0097, de fecha 13.3.2003. Publicado en Diario Oficial de la UE n° C 061 E de 10.03.2004 p. 381-384; y la Resolución del Parlamento Europeo sobre la transmisión de datos personales por las compañías aéreas en los vuelos transatlánticos: estado de las negociaciones con los EE.UU, P5_TA (2003)0429, de fecha 9.10.2003, publicada en el Diario Oficial de la UE nº C 81 E/105 de fecha 31.3.2004.

La Comisión coincidía con el Parlamento Europeo en que resultaba necesario encontrar urgentemente una solución a los problemas derivados de la solicitud de datos de PNR de terceros países y en particular de Estados Unidos.[951] Dicha solución debía ser sólida desde el punto de vista jurídico: que garantizara la protección de los datos personales y la intimidad de los ciudadanos, pero asimismo su seguridad física; estar firmemente ligada a la necesidad de combatir el terrorismo y la delincuencia organizada internacional; poner fin a la incertidumbre jurídica de las compañías aéreas de Europa y del resto del mundo; así como facilitar los viajes con fines legítimos. En estas circunstancias, se celebran los acuerdos que pasamos a analizar.

4.3.2. Acuerdo UE-EE.UU. sobre PNR de 2004, bajo la Directiva 95/46/CE

El primer acuerdo suscrito por la Unión Europea con Estados Unidos de Norteamérica sobre PNR, tuvo como base jurídica el artículo 25 la Directiva 95/46/CE.[952] Este artículo recoge los requisitos para autorizar la transferencia internacional de datos personales desde los Estados Miembros de la Unión Europea a terceros países, la que sólo podrá tener lugar si «el tercer país de que se trate garantice un nivel adecuado de protección».[953] Por tanto, la adecuación del nivel de protección se constituye como un requisito *sine qua non* para que un tercer país pueda ser destinatario de datos obtenidos en la Unión Europea. La Comisión Europea es la facultada para examinar el nivel de protección ofrecido por un tercer país, tomando en cuenta varias circunstancias sobre los datos que se evalúan, decidiendo si un país tercero garantiza un nivel adecuado de protección necesario para la transferencia de los datos personales.[954]

---

[951] El 16 de diciembre de 2003, la Comisión publicó la Comunicación al Consejo y al Parlamento sobre la Transferencia de datos de los registros de nombres de los pasajeros (PNR): un enfoque global de la Unión Europea, con el objetivo de establecer los elementos de un enfoque global de la UE en materia de PNR. pedía un marco legal seguro para las transferencias PNR al Departamento de Seguridad Interior de los EE.UU. *(Department of Homeland Security)* y la adopción de una política interior sobre los PNR. En la Comunicación COM(2003) 826, también propugnaba el desarrollo de un sistema de transmisión *push* de las transferencias de datos por las compañías aéreas y una iniciativa internacional sobre las transferencias de datos PNR que realiza la Organización de la Aviación Civil Internacional (OACI). Disponible online: http://eur-lex.europa.eu/Result.do?idReq=2&page=1 [fecha consulta: 6.1.2014]

[952] Directiva 95/46/CE del Parlamento Europeo y Consejo de la Unión Europea, de 24 de octubre de 1995, relativa a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, publicada en el Diario Oficial de la CE nº L 281, de 23.11.1995. Esta Directiva ha sido modificada por el Reglamento (CE) no 1882/2003 del Parlamento Europeo y del Consejo, publicada en el DO nº L 284 de 31.10.2003, p. 1.

[953] Artículo. 25.1, de la Directiva 95/46/CE.

[954] Ibídem., 25.2. El procedimiento se encuentra regulado en el artículo con arreglo al procedimiento previsto en el artículo 31.2 de la Directiva 95/46/CE.

El 11 de mayo de 2004, el Servicio de Aduanas y Protección de Fronteras de los Estados Unidos (CBP) publicó unos compromisos *(Undertakings)* donde aclara y define las condiciones bajo las cuales se realizaría la transferencia de datos de pasajeros PNR a las autoridades americanas, garantizando que dicha transferencia se harían respetando los principios comunitarios relativos al derecho a la intimidad de las personas.[955] Ello permitió que el 14 de mayo de 2004, la Comisión, mediante la Decisión 2004/535/CE[956], considerara que la CBP garantizaba "un nivel adecuado de protección de datos de los PNR transferidos desde la Comunidad relativos a los vuelos hacia o desde los Estados Unidos.[957] En virtud de esta Decisión de adecuación, el 17 de mayo de 2004, y por la Decisión 496/2004 del Consejo de la Unión Europea, se aprobó la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos sobre el tratamiento y la transferencia de los datos PNR por las compañías aéreas al CBP Estados Unidos.[958] Por último, el 28 de mayo de 2004 los Estados Unidos y la Comunidad Europea firmaron el Acuerdo definitivo que entró en vigor en la fecha de su firma.[959]

Según el Acuerdo, el *procesamiento* y el *tratamiento* por parte del CBP de los datos personales del PNR se regía por la legislación de EE.UU.[960], lo que fue criticado tanto por el Parlamento Europeo como por Supervisor Europeo de Protección de Datos, y el Grupo de Trabajo del artículo 29 sobre protección de datos. También se criticó que el Acuerdo omitía los principios comunitarios esenciales relativos a la protección de datos, y en particular los principios de limitación de la finalidad y proporcionalidad.[961]

---

[955] Publicado en: Federal Register /Vol. 69, No. 131 / Friday, July 9, 2004 /Notices. Disponible en http://www.statewatch.org/news/2004/jul/PNR-Federal-REG-undertakings.pdf [fecha consulta:8.1.2014]

[956] Decisión de la Comisión 2004/535/CE, de 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (*Bureau of Customs and Border Protection*). Publicado en el Diario Oficial de la UE nº L 235 de fecha 6.7.2004

[957] Cfr. artículo 1 de la Decisión de la Comisión 2004/535/CE.

[958] Decisión del Consejo 2004/496/CE, de 17 de mayo de 2004, relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos. Publicada en el Diario Oficial de la UE n° L 183 de 20/05/2004, p. 83

[959] Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos PNR por las compañías aéreas al Departamento de Seguridad Nacional, Oficina de Aduanas y Protección Fronteriza. Publicado en el Diario Oficial de la UE nº L 142M de 20.5.2004, p. 50.

[960] Decisión de la Comisión 2004/535/EC, Párrafo 1.

[961] Al respecto véase Michael NINO, ob. cit., pp. 71, y la bibliografía citada por la autora.

En cuanto a los *fines* para el procesamiento de datos se refiere, los datos del PNR podían ser utilizados por el CBP, a fin de «prevenir y combatir: 1. terrorismo y delitos conexos; 2. otros delitos graves, incluida la delincuencia organizada, 3. la fuga de orden de arresto o detención por esos delitos los crímenes».[962] Como se puede apreciar, la redacción de la categoría nº 2 era tan vaga que podía incluir actividades delictivas no relacionadas con los actos terroristas y, por tanto, la transmisión de datos no autorizados, lo que atentaría contra el principio de limitación de objetivos o finalidades. Como ya hemos indicado, es fundamental que la lucha contra el terrorismo internacional sea limitada y definida, ya que unos fines tan amplios podrían ocasionar limitaciones injustificadas del derecho a la privacidad y las libertades fundamentales.

En cuanto a los **tipos de datos** del PNR que se transfieren, se dispuso que la transferencia de datos incluyera una lista de treinta y cuatro elementos. El esquema original del Acuerdo, incluía el traspaso de treinta y ocho datos de los PNR, por tanto, hubo una reducción cuantitativa de los datos a transmitir. No obstante, el número y la cantidad de datos a transferir en el marco del Acuerdo de 2004 se mantuvo muy amplio, por lo que la transferencia no podía calificarse de suficiente y pertinente de acuerdo con los principios consagrados en el artículo 6 de la Directiva 95/46/CE.[963] Como regla general, la transmisión de datos sensibles protegidos por el artículo 8 de la Directiva 95/46 fue excluida. Respecto de la **duración** de la retención de datos, el Acuerdo dispuso que la CBP pudiera mantener y acceder a los datos PNR de los pasajeros durante tres años y seis meses, un tiempo de retención de datos excesivo y que no cumple con el principio de proporcionalidad. Por último, el **método** de la transferencia de datos elegido fue el sistema *pull*, según el cual las autoridades de los EE.UU. podrían acceder al sistema de reservas de la compañía aérea y copiar los datos requeridos en su propia base de datos.[964] Esta técnica se prefirió al sistema de protección *push*, por el cual las compañías aéreas transmiten los datos PNR requeridos a la base de datos de la

[962] Cfr. Considerando (15) de la Decisión de la Comisión 2004/535/CE.
[963] En el mismo sentido, véase el Dictamen 4/2003, pp. 6-7.
[964] Párrafo 1 de la Decisión del Consejo 2004/496/CE, de 17 de mayo de 2004, relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos. Publicada en el Diario Oficial de la UE n° L 183 de 20/05/2004, p. 83.

autoridad requirente, es decir, la compañía aérea transmite los datos al tercer país sin permitir el acceso de estos a sus bases de datos.[965]

4.3.3. La Sentencia del Tribunal Europeo de Justicia que anula los Acuerdos

El 27 de julio de 2004, el Parlamento Europeo, con el apoyo de la Supervisor Europeo de Protección de Datos, interpuso dos recursos ante el Tribunal de Justicia de las Comunidades Europeas (asunto C-317/2004 y C-318/2004) que se acumularon posteriormente, con el fin de solicitar la anulación de la Decisión 2004/496/CE relativa a la celebración del acuerdo entre la UE y EE.UU sobre transferencia de datos del PNR a la CPB, y la Decisión 2004/535/CE sobre el carácter adecuado de la protección por parte de la CPB.

En su sentencia de 30 de mayo de 2006, el TJCE anuló ambas Decisiones, la primera del Consejo y la segunda de la Comisión.[966] En sus argumentos, que recogió gran parte de las conclusiones del Abogado General Léger,[967] señala que «la transferencia de los datos de los PNR al CBP constituye un tratamiento que tiene por objeto la seguridad pública y las actividades del Estado en materia penal».[968] Desarrollando el punto, indica que si bien es correcto que los datos del PNR son

---

[965] Un definición similar se puede encontrar en la Comunicación de la Comisión COM(2010) 492 final, sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países, COM(2010) 492 final, de fecha 21.9.2010, , p. 2

[966] Sentencia del Tribunal de Justicia, en los asuntos acumulados C-317/04 y C-318/04, "*Parlamento Europeo/Consejo de la Unión Europea y Parlamento Europeo/Comisión de las Comunidades Europeas",* de fecha 30.5.2006. El texto íntegro se encuentra en el sitio de Internet del Tribunal de Justicia http://curia.eu.int/jurisp/cgi-bin/form.pl?lang=ES&Submit=rechercher&numaff=C-317/04 et C-318/04 Para un análisis de la sentencia véase L. GONZÁLEZ "El Tribunal de Justicia de las Comunidades Europeas anula el Acuerdo entre la Comunidad Europea y los EE.UU. para la transmisión de los datos sobre los pasajeros por las compañías aéreas", *Revista española de Derecho Europeo*, n° 20 (2006), pp. 557-576; y G. Gilmore *et al.*, 'Court of Justice: Joined Cases C-317/04 and C-318/04, European Parliament v. Council and Commission', 2007 *Common Market Law Review*, no. 4, pp. 1081-1099. Asimismo puede consultarse: Ángel RODRÍGUEZ-VERGARA DÍAZ, "Derechos fundamentales, lucha antiterrorista y espacio europeo de libertad, seguridad y justicia (de nuevo en torno a las listas antiterroristas y la intimidad de los usurarios de líneas aéreas)", *Revista de Derecho de la Unión Europea*, n.10. 1er semestre 2006. pp.223-229; Cristian ORÓ MARTÍNEZ, "La anulación de la transferencia de datos personales de los pasajeros aéreos a los Estados Unidos. Comentario de la sentencia del TJCE de 30 de mayo de 2006, C-317/04 y C-318/04, Parlamento Europeo contra Consejo de la Unión Europea y Parlamento Europeo contra Comisión de las Comunidades Europeas", *Revista General de Derecho Europeo*, núm. 11, 2006, Iustel, edición electrónica.

[967] Véase las Conclusiones del Abogado General Léger, de fecha 22 noviembre de 2005. El texto íntegro de las conclusiones se puede encontrar en el sitio de Internet del Tribunal de Justicia: http://curia.eu.int/jurisp/cgi-bin/form.pl?lang=es

[968] Cfr. el apartado nº 56 de la Sentencia del TJCE.

recogidos inicialmente por las compañías aéreas en el marco de una actividad comprendida en el ámbito del Derecho comunitario (venta de un billete de avión), también lo es que el tratamiento de los datos contemplado en la Decisión de adecuación tenga una naturaleza distinta. Agrega que en efecto «el tratamiento de datos a que se refiere esta Decisión no es necesario para la realización de una prestación de servicios, sino que se considera necesario para salvaguardar la seguridad pública y para fines represivos».[969] En la misma línea, señaló que en la sentencia del caso Lindqvist el Tribunal declaró «que las actividades que se mencionan como ejemplos en el artículo 3, apartado 2, primer guión de la Directiva (95/46/CE) son, en todos los casos, actividades propias del Estado o de las autoridades estatales y ajenas a las esfera de actividades de los particulares», [970] agregando que «no obstante, de ello no se desprende que, debido al hecho de que los datos de los PNR sean recogidos por operadores privados con fines mercantiles y de que sean éstos quienes organizan su transferencia a un Estado tercero, dicha transferencia no esté incluida en el ámbito de aplicación de la citada disposición. En efecto, esta transferencia se inserta en un marco creado por los poderes públicos y cuyo objetivo es proteger la seguridad pública».[971] A nuestro juicio ésta es la aportación más relevante de la sentencia, ya que utiliza como criterio diferenciador para determinar la legislación aplicable, la **finalidad** y el **uso** que se da a los datos sin importar si estos en su origen fueron recogidos con un propósito distinto.

Por otra parte, sobre la Decisión 2004/496 el Tribunal señala que «el artículo 95 CE en relación con el artículo 25 de la Directiva (95/46/CE) no puede constituir la base de la competencia de la Comunidad para celebrar el Acuerdo».[972] En efecto, este Acuerdo se refiere a la misma transferencia de datos que la Decisión sobre el carácter adecuado de la protección y, por tanto, a tratamientos de datos que, como ya se ha expuesto anteriormente, no están comprendidos en el ámbito de aplicación de la Directiva.[973]

Se ha criticado la sentencia del Tribunal de Justicia, por centrar su atención en aspectos de procedimiento, tales como las relativas al ámbito de aplicación de la

[969] Ibídem apartado nº 57.
[970] Cfr. apartado 43, de la sentencia del TJCE, de fecha 6 de noviembre de 2003 (Asunto C-101/01- Bodil Lindqvist).
[971] Cfr. apartado 58 de la sentencia en estudio.
[972] Ibídem, apartado 68.
[973] Ídem.

Directiva 95/46 y la competencia de la Comunidad para celebrar un acuerdo de una zona específica con arreglo al artículo 95 TCE, sin pronunciarse sobre otros temas, tanto sustantivos como de procedimiento importantes, propuestos por el Parlamento Europeo en su demanda y examinados por el Abogado General Léger, tales como los efectos de las resoluciones impugnadas en el ejercicio del derecho a la intimidad de las personas.[974] También se criticó que la sentencia del Tribunal de Justicia ha dado lugar a la anulación del Acuerdo y, por lo tanto, a la eliminación de los efectos negativos sobre el derecho a la intimidad derivadas de la aplicación de dicho Acuerdo, pero no contribuyó a garantizar la seguridad jurídica a largo plazo, ya que no se llegó a una solución definitiva y clara a los problemas planteados por el Acuerdo.[975] Esto creó una situación de inseguridad jurídica que llevó primero a un Acuerdo provisional, y luego al Acuerdo de 2007, los cuales, como veremos, contienen disposiciones cuestionables sobre limitación de los principios fundamentales del derecho a la intimidad y de la protección de datos personales.

4.3.4. El Acuerdo provisional de 2006

En octubre de 2006, después de la conclusión de las negociaciones entre la Comisión y los Estados Unidos, el Consejo de la UE aprobó un Acuerdo provisional entre ambas partes sobre el tratamiento y la transferencia de datos del PNR desde la Unión Europea a las autoridades estadounidenses.[976] Este Acuerdo sustituyó al de 2004 y expiró el 31 de julio de 2007 para ser sustituido por un acuerdo definitivo.[977]

Entre las principales características de este Acuerdo provisional podemos mencionar la ampliación de las autoridades norteamericanas habilitadas para el

[974] En el mismo sentido véase Michele NINO, ob. cit., pp. 73-74.
[975] Ídem.
[976] Decisión 2006/729/PESC/JAI del Consejo, de 16 de octubre de 2006, relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos. Publicado en el Diario Oficial de la UE nº L 298 de 27.10.2006, p. 27/28
[977] Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos. Hecho en Luxemburgo, el 16 de octubre de 2006, y en Washington, el 19 de octubre de 2006. Publicado en el Diario Oficial de la UE nº L 298 de 27.10.2006, p. 29/31

tratamiento de los datos del PNR. A diferencia del acuerdo anterior, en el que solo se permitía el acceso al Servicio de Aduanas y Protección de Fronteras *(Bureau of Customs and Border Protection),* este Acuerdo permite el acceso a los datos a otras Agencias del Departamento de Seguridad del Territorio Nacional (*Department of Homeland Security*), como lo son la Autoridad de Inmigración y Aduanas de los Estados Unidos *(U.S. Immigration and Customs Enforcement)* y la Oficina del Secretario *(Office of the Secretary)*, así como a los organismos de apoyo directo a estas Agencias.[978] El acuerdo mantiene el sistema de transmisión de datos *(pull)* que permite a las autoridades norteamericanas acceder electrónicamente a los datos del PNR disponibles en el sistema de reservas de las compañías aéreas y copiar los mismos en su propia base de datos.[979]

El nuevo Acuerdo no contenía una indicación precisa de los datos del PNR que serían objeto del tratamiento y la transferencia. Por otra parte, el Acuerdo establecía que el tratamiento y la transferencia de datos se haría "teniendo en cuenta las normas y reglamentaciones de los Estados Unidos",[980] y sólo se refería el artículo 6, apartado 2, del Tratado de la Unión Europea sobre el respeto de los derechos fundamentales y, en particular, al derecho conexo relativo a la protección de los datos personales.[981]

Como se puede apreciar, la indefinición de los datos del PNR que se transfieren, el mantenimiento de un método de transferencia de datos más susceptibles a poner en peligro la protección de la intimidad y la expansión de las entidades facultadas para tener acceso directo a los datos del PNR conservados por las compañías aéreas, muestran que las normas de la Acuerdo de 2006, por ser menos precisas y detalladas que las del Acuerdo de 2004, permitían más abusos y violaciones a las derechos fundamentales de las personas.[982]

[978] Ídem, párrafo 2º.
[979] Ibídem, párrafo 4º.
[980] Ídem.
[981] Ibídem, párrafo 5º.
[982] Al respecto véase Michele NINO, ob. cit., p. 75 y bibliografía citada por la autora.

4.3.5. El Acuerdo definitivo de 2007 entre la UE y EE.UU sobre transferencia de datos del PNR

Mediante su Decisión de 23 de julio de 2007, el Consejo de la Unión Europea aprobó la celebración de un nuevo acuerdo sobre el tratamiento y la transferencia de datos PNR que sustituye al Acuerdo provisional celebrado en 2006.[983] El Acuerdo consiste en el propio documento y una carta de EE.UU. a la UE donde se explica las modalidades de almacenamiento, uso y transferencia de datos PNR por parte del Departamento de Seguridad del Territorio Nacional (*Department of Homeland Security*).[984]

En cuanto a los fines de las transferencia de datos del PNR, el Título I de la carta señala que las autoridades de EE.UU. pueden utilizar los datos del PNR, «con el propósito de prevenir y combatir: 1) el terrorismo y los delitos asociados, 2) otros graves delitos de carácter transnacional, incluida la delincuencia organizada, y 3) la fuga en caso de orden de arresto o pena de reclusión por los delitos anteriormente mencionados».[985] Además, las autoridades norteamericanas pueden utilizar y procesar los datos del PNR con el fin de proteger «los intereses vitales del interesado o de otras personas, o en todo procedimiento judicial penal, o cuando lo exija la ley».[986]

Como acertadamente ha señalado el Grupo del artículo 29, «los fines que justifican la transferencia de datos, incluidas las numerosas excepciones, no están lo suficientemente especificados y sobrepasan los contemplados por la normativa sobre

[983] Decisión 2007/551/PESC/JAI del Consejo, de 23 de julio de 2007, relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos. Publicado en el Diario Oficial de la UE nº L 204 de 4.8.2007, p. 16/17.
[984] Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (Acuerdo PNR 2007).
[985] Cfr. el Titulo I, de la Carta de los EE.UU. a la UE, anexa al Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (Acuerdo PNR 2007). Publicada en el Diario Oficial de la UE nº L 204 de 4.8.2007, p. 21. La cita corresponde a una traducción realizada por los autores, que se puede contrastar con versión original en inglés, disponible en http://www.dhs.gov/xlibrary/assets/pnr-2007agreement-usltrtoeu.pdf [fecha consulta 11.1.2014].
[986] Ídem.

protección de datos».[987] Por otra parte, el Acuerdo no establece definiciones «en cuanto al significado de los delitos vinculados al terrorismo y los delitos graves de carácter transnacional, incluida la delincuencia organizada, lo que deja un gran margen a la interpretación».[988] La vaguedad de los fines indicados puede legitimar un uso generalizado de los datos del PNR, que no cumplan con la limitación de la finalidad y calidad de los datos y los principios de proporcionalidad. El hecho de que los datos PNR también pueden ser utilizados en cualquier procedimiento judicial penal, o según lo requiera la ley de EE.UU. es preocupante, ya que las autoridades norteamericanas podrían decidir el uso y tratamiento de datos de los PNR para otros delitos menos graves que el terrorismo o la delincuencia organizada, poniendo en riesgo el derecho personal a la privacidad.[989]

En cuanto a los elementos de datos que se transfieren, del Acuerdo de 2007 reduce la cantidad de datos a diecinueve elementos a transmitir, es decir, hay una disminución cuantitativa respecto del Acuerdo de 2004, que incluía treinta y cuatro elementos.[990] No obstante, esta reducción no implica una menor afectación del derecho a la intimidad, ya que cualitativamente la variedad de los datos transmisibles aumenta.[991] También se permite, en un caso excepcional, que las autoridades de EE.UU. puedan acceder y utilizar los datos sensibles (que indiquen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a un sindicato o el estado de salud o la vida sexual del viajero), actividad que fue excluida en el marco del Acuerdo de 2004.[992] En consecuencia, se critica que la cantidad de información que las autoridades de EE.UU. pueden obtener y procesar es muy amplia y no es proporcional a los objetivos perseguidos por el Acuerdo.

---

[987] Dictamen 5/2007 del Grupo de Trabajo del artículo 29, relativo al nuevo Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por parte de las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, celebrado en julio de 2007.
[988] Ídem.
[989] En el mismo sentido véase Michele NINO, op. cit., p 76. y bibliografía citada por la autora.
[990] Véase el Título III de la Carta anexa al Acuerdo PNR 2007.
[991] En este sentido véase la Resolución del Parlamento Europeo, de 12 de julio de 2007, sobre el acuerdo PNR con los Estados Unidos de América. Publicado en el Diario Oficial de la UE nº C 175 E de fecha 10.7.2008, p. 564, punto 18.
[992] La forma, plazo y condiciones de acceso a los datos sensible, se regula en el Titulo III de la Carta de los EE.UU. a la UE, anexa al Acuerdo de 2007.

Respecto de las autoridades norteamericanas autorizadas para la recepción y tratamiento de los datos del PNR, ha habido un incremento. En efecto, el Acuerdo de 2004 identificó un número limitado de organismos dentro de Seguridad Nacional que tenían derecho a recibir los datos del PNR. En cambio, el Acuerdo de 2007 establece que el Departamento de Seguridad Nacional (*Department of Homeland Security*, DHS) puede procesar los datos PNR que reciba de la Unión Europea y «tratar a los interesados afectados por dicho tratamiento de conformidad con las leyes de EE.UU.», de tal modo que no identifica expresamente a los organismos específicos facultados para acceder a los datos del PNR, ampliando de manera general y desproporcionada las entidades con derecho a tener acceso a datos personales de los pasajeros.[993]

En cuanto al tiempo de retención de los datos, éste se ha ampliado de tres años y medio (Acuerdo de 2004) a quince años en el Acuerdo de 2007. Los datos del PNR se conservan durante siete años en una base de datos activa y, posteriormente, se trasladan a una base de datos inactiva por el resto del periodo.[994] Se ha señalado que este tiempo de retención de datos parece desproporcionada y excesiva en relación con los fines a alcanzar y puede plantear problemas con el cumplimiento de los principios comunitarios de proporcionalidad y limitación de los fines, así como con el artículo 8 de la CEDH.[995]

En cuanto al método de transferencia de datos, el Acuerdo de 2007 ha sustituido el sistema o método de transferencia *pull* previsto por el Acuerdo de 2004 por el sistema *push.*[996] De esta manera, las autoridades de EE.UU. no tienen acceso directo a los datos del PNR, sino que reciben la información de las compañías aéreas. Sin embargo, el Acuerdo establece que el sistema de *pull* se mantiene en efecto en caso que las compañías aéreas no pueden aplicar el sistema de *push.*[997]

La utilización el sistema *push* es uno de los aspectos positivos del nuevo acuerdo, ya que permite un mejor control de las autoridades de EE.UU. por parte de las autoridades europeas y reduce los riesgos de invasión excesiva a la privacidad de los pasajeros. Sin embargo, la posible coexistencia de ambos sistemas no sólo puede

[993] Véase el Título II. de la Carta de los EE.UU. a la UE, anexo al Acuerdo de 2007.
[994] Ibídem, Titulo VII.
[995] Al respecto véase la Resolución del Parlamento Europeo de 12.7.2007, Punto 18.
[996] Cfr. Título VIII de la Carta de los EE.UU. a la UE, anexo al Acuerdo de 2007.
[997] Ídem.

legitimar posibles violaciones del derecho de los pasajeros aéreos a la intimidad, sino también podría causar una "distorsión de la competencia entre compañías aéreas de la UE".[998]

En cuanto a la ley aplicable al tratamiento y transferencia de los datos personales desde la Unión Europea a los Estados Unidos, el Acuerdo de 2007 los somete exclusivamente a las leyes estadounidenses. Según el Acuerdo, el DHS puede procesar y utilizar los datos del PNR, «de conformidad con las leyes de EE.UU.»[999] y la UE no puede «interferir con las relaciones entre Estados Unidos y terceros países para el intercambio de información a los pasajeros por razones de protección de datos».[1000] Se ha señalado que la dependencia de la Unión Europea sobre las leyes de EE.UU. constituye una señal peligrosa, ya que no existe un marco legal de carácter general en los EE.UU. que establezca criterios generales aplicables a todo tipo tratamiento de datos personales.[1001] El Acuerdo no tiene plenamente en cuenta la existencia de contradicciones entre el Derecho comunitario y las leyes de EE.UU. sobre el tratamiento de datos personales, lo que podría poner en peligro el ejercicio de los distintos derechos protegidos por la Unión.

En resumen, el Acuerdo de 2007, aunque formalmente reduce el número de datos transmisibles, permite adoptar el sistema *push* de transmisión de datos, y establece un sistema de revisión periódica desde su implementación. Lo cierto es que esta medida establece una serie de mayores limitaciones al derecho a la privacidad en general y a la protección de datos en particular respecto (o en comparación con) al Acuerdo de 2004, aunque no cumplen con las normas comunitarias sobre el derecho a la privacidad.[1002] Por tanto, es necesario que el Acuerdo sea modificado y se establezca una definición más clara respecto de los propósitos que se persiga; una evaluación coherente y adecuada de los datos que se transfieren; una identificación clara de las autoridades facultadas para recibir los datos; una aplicación uniforme del sistema *push*, y una referencia clara y vinculante a los principios comunitarios en materia de derecho a la intimidad.

---

[998] Al respecto véase el punto 8 de la Resolución del Parlamento Europeo de 12.7.2007.
[999] Véase el párrafo 3 del Acuerdo PNR de 2007.
[1000] Ibídem, párrafo 6.
[1001] En el mismo sentido, véase Michele NINO, op. cit., p. 77.
[1002] Ídem.

4.3.6. El Acuerdo de 2005 sobre la transferencia de los datos API/PNR entre la Unión Europea y Canadá

El Acuerdo entre la Unión Europea y Canadá, sobre los datos API/PNR constituye otro de los grandes Convenios internacionales suscritos por la Unión sobre transferencia internacional de datos del PNR a terceros países por razones de seguridad.[1003] Durante el proceso de elaboración, la propuesta de Acuerdo fue objeto de algunas observaciones por parte del Grupo de Trabajo del artículo 29, donde se señalaba que algunas de sus disposiciones atentaban en contra de la privacidad y la protección de los datos personales.[1004] Tras las negociaciones entre la Unión Europea y representantes de Canadá, las autoridades canadienses cumplieron con los requisitos impuestos por la Unión Europea, modificándose la propuesta original y estableciendo compromisos al respecto.

El Acuerdo establece que la transferencia y el tratamiento de los datos personales API/PNR provenientes de la Unión Europea, estarán regulados por las condiciones establecidas en los "Compromisos"[1005] de la Agencia de Servicios de Fronteras de Canadá (*Canada Border Services Agency*, en adelante CBSA*)* en relación con la aplicación de su programa sobre el PNR, así como por la legislación nacional canadiense sobre la materia. Por tanto, el fundamento jurídico para el tratamiento de los datos personales API/PNR con fines represivos por parte de Canadá, lo encontramos en su propia legislación y en los Compromisos pactados sobre la materia con la Unión Europea.[1006] En cuanto al método de transferencia de datos se refiere, se ha adoptado el

[1003] Acuerdo entre la Comunidad Europea y el Gobierno de Canadá, firmado en Luxemburgo el 3 de octubre de 2005, sobre el tratamiento de datos procedentes del sistema de información anticipada sobre pasajeros y de los expedientes de pasajeros. Publicado en el Diario Oficial de la UE nº L 82 de 21.3.2006, p. 14/19 y en vigor desde el 22.3.2006.

[1004] Dictamen 3/2004 del Grupo del Trabajo del artículo 29, sobre el nivel de protección garantizado por Canadá para la transmisión de datos de pasajeros y de la Información Avanzada de Pasajeros de las compañías aéreas, WP 88, de fecha 11.2.2004, disponible en línea en su versión en ingles: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp88_en.pdf [fecha consulta 16.11.2010]

[1005] Véase la Decisión de la Comisión 2006/253/CE, de 6 de septiembre de 2005, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros (Passenger Name Records, PNR) que se transfieren a la *Canada Border Services Agency* (Agencia de Servicios de Fronteras de Canadá) y el Anexo, con los Compromisos de la Agencia Canadiense de Servicios Fronterizos en relación con la aplicación de su Programa de PNR. Publicado en el Diario Oficial de la UE nº L 91 de 29.3.2006

[1006] El Anexo a la Decisión de la Comisión 2006/253/CE, señala que del derecho de la CBSA a obtener y recopilar dicha información se halla en el apartado 107.1 de la Ley de Aduanas *(Customs Act)* y en los

sistema *push*, mediante la creación de un Sistema de Información sobre Pasajeros (denominado PAXIS), por medio del cual, las compañías aéreas envían a la CBSA los datos de la API y del PNR.[1007] Este sistema debería permitir menos abusos y un control de mayor calidad sobre el flujo de datos personales de los pasajeros aéreos, con la consiguiente protección de su privacidad, ya que serán las compañías aéreas quienes transferirán los datos, no estando obligadas a permitir que las autoridades canadienses tengan acceso directo a los mismos.

En cuanto a los datos que deben recopilarse y enviarse a la CBSA, el Acuerdo contiene una lista de veinticinco elementos.[1008] Estos son cualitativamente más limitados, ya que excluye los datos sensibles y todos los campos de texto abierto u observaciones generales.[1009] Esto constituye un avance respecto de los acuerdos suscritos con los Estados Unión, como ha reconocido el Parlamente Europeo,[1010] ya que por una parte excluye la transmisión de datos sensibles, cumpliendo así con el artículo 8 de la Directiva 95/46, y por otra, evita la transferencia general de datos personales. También es positiva la exclusión de la transmisión de categorías abiertas de los datos, ya que "estas categorías pueden generar confusión o resultar engañosas respecto a aspectos sensibles de la conducta de los pasajeros y de las personas que los acompañan".[1011] En la misma línea, el Grupo del Artículo 29 y el SEPD ha acogido con satisfacción la lista de datos del PNR que se transfieren en virtud del Acuerdo, no obstante haber expresado algunas dudas compartidas. El primero ha puesto de relieve que no todos los datos que deben recogerse pueden considerarse como legítimos y no excesivos a la luz del derecho comunitario.[1012] El Supervisor Europeo de Protección de

---

Reglamentos (sobre aduanas) relativos a la información de los pasajeros *[Passenger Information (Customs) Regulations]* adoptados con arreglo a la misma, y en el apartado 148.1.d) de la Ley de protección de la inmigación y los refugiados *(Immigration and Refugee Protection Act)* y en el Reglamento 269 de los Reglamentos de protección de la inmigración y los refugiados *(Regulation 269 of the Immigration and Refugee Protection Regulations)* adoptado con arreglo a dicha normativa.

[1007] Véase el punto 7 de los Acuerdos.

[1008] Cfr. Anexo A del la Decisión de la Comisión 2006/253/EC.

[1009] Ibídem., punto nº 4.

[1010] Informe Final A6-0226/2005, del Parlamento Europeo, sobre la propuesta de Decisión del Consejo relativa a la celebración de un Acuerdo entre la Comunidad Europea y el Gobierno de Canadá sobre el tratamiento de datos procedentes del sistema de información anticipada sobre pasajeros (API) y de los expedientes de los pasajeros (PNR) (COM(2005)0200 – C6-0184/2005 – 2005/0095(CNS)), de 4.7.2005, disponible en http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//NONSGML+REPORT+A6-2005-0226+0+DOC+PDF+V0//ES [fecha consulta: 18.11.2010]

[1011] Ibídem, p. 10.

[1012] Dictamen 1/2005 del Grupo de Trabajo del artículo 29, sobre el nivel de protección garantizado por Canadá para la transmisión del PNR e información previa sobre pasajeros procedente de las compañías aéreas, aprobado por el Grupo el 19 de enero de 2005, p. 4.

Datos, por su parte, ha declarado que la transferencia de determinadas categorías de datos puede dar lugar a problemas en cuanto a la protección del derecho a la intimidad, en particular la información sobre programas de fidelización, que podría revelar datos sobre el comportamiento del viajero y toda la información recopilada del sistema API, que contiene gran parte de los datos que figuran en el pasaporte del viajero.[1013]

En cuanto al tiempo de retención de datos, los compromisos establecen un período de tres años y medio para los datos personales relativos a una persona que no sea objeto de una investigación en Canadá.[1014] Este término parece estar en el cumplimiento de los principios de proporcionalidad y calidad de los datos previstos por el Derecho comunitario. No obstante, si la persona es objeto de una investigación en Canadá por alguno de los motivos contemplados en el Acuerdo, este plazo se ampliará a seis años.[1015]

Respecto a las transferencias posteriores de datos a otras autoridades canadienses o a terceros países, los Compromisos establecen que sólo permiten la transferencia de una cantidad mínima de datos en casos específicos relacionados con el terrorismo o con delitos relacionados con el terrorismo, como también, que ellos sólo se compartirán con un país objeto de una decisión de idoneidad con arreglo a la Directiva (95/46/CE) o incluido por ella.[1016] La forma como se encuentra regulado este punto constituye un avance significativo, ya que establece las materias, formas y circunstancias en que se pueden dar dichas transferencias posteriores. Lo mismo creemos sobre la exigencia de que el país que recibe la información asegure un nivel adecuado de protección del derecho a la intimidad, factor clave para garantiza que el flujo de información transferida respete dicho derecho.

[1013] Dictamen del Supervisor Europeo de Protección de Datos, sobre la propuesta de decisión del Consejo relativa a la celebración de un Acuerdo entre la Comunidad Europea y el Gobierno de Canadá sobre el tratamiento de datos procedentes del sistema de información anticipada sobre pasajeros (API) y de los expedientes de los pasajeros (PNR) (COM(2005) 200 final). Publicado en el Diario Oficial de la UE nº C 218 de 6.9.2005, p. 6. Disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2005:218:0006:0010:ES:PDF

[1014] Véase el apartado 8 de los Compromisos.

[1015] Ibídem., apartado 9.

[1016] Ibídem., apartados 2-15 (sobre transferencias posteriores a otros organismos canadienses) y apartados 16-19 (sobre transferencias posteriores a otros países).

El Acuerdo entre Canadá y la Unión Europea sobre la transferencia de datos API /PNR se acogió de manera positiva, ya que protege la privacidad de los pasajeros de mejor manera que lo hacen los Acuerdos UE-EE.UU. Ello obedece a diversas razones. En primer lugar, Canadá cuenta con un sistema legislativo de protección de la privacidad y los datos de carácter personal que constituye una condición esencial para cualquier injerencia sobre el derecho a la intimidad.[1017] Asimismo, cuenta con una autoridad independiente (el Comisario de Datos) similar al sistema europeo previsto por la Directiva 95/46 y el artículo 286 TCE.[1018] La Ley de protección del derecho a la intimidad de Canadá otorga a las personas físicas los derechos de acceso, rectificación y oposición respecto a toda información personal que les ataña, derechos que se extienden a las personas cuyos datos son transferidos en virtud de los Compromisos suscritos.[1019]

No obstante lo anterior, también se han formulados observaciones al Acuerdo, que deberían ser corregidos al momento de la renovación o renegociación de un nuevo Acuerdo.[1020] En primer lugar, el nuevo Convenio debería establecer una definición más acabada de los fines para los que se permite la transferencia de los datos personales de los pasajeros. La sección 2 permite la transferencia de los datos relativos a personas que tengan una relación con el terrorismo o delitos relacionados con el terrorismo u otros delitos graves, incluida la delincuencia organizada, que tengan carácter transnacional.[1021] Sobre este punto, se han pronunciado tanto el Grupo de Trabajo del artículo 29 como el SEPD. El primero ha señalado que los fines están bien definidos y "guarda una clara relación con la lucha contra los actos terroristas.[1022] En la misma línea el SEPD ha señalado que esta limitación de los fines, en sí misma, no infringe lo dispuesto en la Directiva, ni los principios subyacentes en la misma.[1023] No obstante, algunos autores, señalan que el término "delito grave" es tan vago que permite a la CBSA utilizar y procesar los datos para fines no propiamente relacionados con el terrorismo.[1024] De esta manera, el derecho a la intimidad podría verse en peligro debido

[1017] En el sistema Europeo, esta exigencia constituye la condición esencial presente tanto en el artículo 8 de la Carta Europea de Derechos Humanos, como por el artículo 8 del Convenio Europeo de Derechos Humanos (CEDH).
[1018] Véase el Informe Final del Parlamento Europeo A6-0226/2005, p. 10.
[1019] Ídem.
[1020] Sobre este punto, véase Michele.NINO, op. cit., p. 79.
[1021] Véase el apartado 2 de los Compromisos.
[1022] Dictamen 1/2005 del Supervisor europeo de protección de datos, p. 4.
[1023] Ibídem, párrafos 24 y 25.
[1024] Al respecto, véase Michele NINO, op. cit., p. 79.

a la definición poco clara de los efectos según el cual la transferencia de datos PNR se admite, permitiendo posibles abusos por las autoridades canadienses. Además, algunas categorías de datos como información de viajero frecuente y la información APIS, cuyo tratamiento no sea necesario y que no cumplan con los principios de proporcionalidad y de limitación de objetivos, debe ser eliminado de la lista de los PNR que se transfieren.[1025] Como se puede apreciar, éstas son las mismas críticas que se formularon a los Acuerdos con Estados Unidos, por lo que creemos debe ser un punto a estudiar con mayor detención de cara a la renovación o suscripción de nuevos Acuerdos sobre transferencia internacional de datos API/PNR con fines de prevención/represión de actos terroristas.

4.3.7. El Acuerdo de 2008 sobre el PNR entre la Unión Europea y Australia

Después de los Acuerdos suscritos por la Unión Europea con Estados Unidos y Canadá, ésta firmó un Acuerdo con Australia sobre el tratamiento y transferencia de los datos contenidos en el registro de nombres de los pasajeros (PNR) que gestionan las compañías aéreas a los Servicios de Aduanas de Australia (en adelante, SAA).[1026]

El objeto de este Acuerdo son los datos del PNR originados en la UE sobre los pasajeros con destino Australia, procedentes de ese país o con escala en él.[1027] Según este Acuerdo, la transferencia y tratamiento de datos del PNR de la Unión Europea, originados por las compañías aéreas al servicio de aduanas australiano, se rige por la legislación australiana. Respecto del nivel de protección que brinda la legislación australiana a los datos de carácter personal transferidos en virtud del Acuerdo, el Grupo de Trabajo del artículo 29 señaló que la legislación de éste país garantiza un nivel adecuado de protección de la privacidad de las personas, de conformidad con el Derecho comunitario.[1028]

[1025] Ídem.

[1026] Acuerdo entre la Unión Europea y Australia sobre el tratamiento y la transferencia de datos, generados en la Unión Europea, del registro de nombres de los pasajeros (PNR) por las compañías aéreas a los Servicios de Aduanas de Australia. Publicado en el Diario Oficial de la UE nº L 213 de 8.8.2008, p. 49/57. Disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:213:0049:0057:ES:PDF

[1027] Ibídem., apartado 1 del Anexo.

[1028] Dictamen 1/2004 del Grupo de Trabajo del artículo 29, sobre el nivel de protección garantizado por Australia en la transmisión de datos del registro de nombres de pasajeros de las compañías aéreas,

En cuanto la finalidad del tratamiento de los datos del PNR generados en la Unión Europea por parte del Servicio de Aduanas Australiano, el Acuerdo señala que éste puede tratar los datos con el fin de prevenir y combatir: " i) el terrorismo y delitos afines al terrorismo; ii) los delitos graves de carácter transnacional, como la delincuencia organizada; iii) la huida ante órdenes judiciales o autos de privación de libertad por los delitos mencionados."[1029] Luego agrega que los datos del PNR también pueden ser tratados por el SAA "cuando sea necesario para la protección de los intereses vitales del titular de los datos o de otros"[1030] o "por resolución judicial o en virtud del Derecho australiano".[1031] Así, el Servicio de Aduanas Australiano está autorizado, en virtud del Acuerdo, para tratar y transferir información del PNR para casos no relacionados con la prevención y la lucha contra el terrorismo, lo que atentaría contra el principio de limitación de los fines. Por ello sería recomendable restringir, definir y acotar los fines para los cuales se transfiere los datos del PNR de cara a una próxima renovación del Acuerdo, o por el contrario, suscribir un Acuerdo más amplio que abarque y regule la transferencia internacional de datos personales en el marco de la cooperación policial y judicial. En este último caso, se debe establecer el marco regulatorio adecuado para permitir la transferencia de datos con el fin de prevenir, investigar, detectar o perseguir delitos, incluido el terrorismo, pero respetando los derechos y libertades fundamentales de las personas afectadas, en particular su privacidad y la protección de sus datos personales.[1032]

Respecto al tiempo de retención de datos, el Acuerdo establece que "las Aduanas conservarán los datos del PNR generados en la UE un máximo de tres años y medio desde la fecha en que los hayan recibido y una vez transcurrido ese plazo los datos podrán quedar archivados dos años más".[1033] En principio, un plazo de retención de datos de cinco años y medio podría considerarse adecuado, no obstante, el problema es

---

adoptado el 16 de enero de 2004, pp. 13-15. Disponible en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp85_es.pdf [fecha consulta: 23.11.2010]

[1029] Artículo 5.1 del Acuerdo sobre PNR entre la UE y Australia.

[1030] Ibídem., artículo 5.2

[1031] Ibídem., artículo 5.3

[1032] Al respecto véase la Propuesta de Resolución del Parlamento Europeo, de 3.11.2010, sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países y las Recomendaciones de la Comisión al Consejo para autorizar la apertura de negociaciones para un Acuerdo entre la Unión Europea y Australia, Canadá y los Estados Unidos.

[1033] Párrafo 12 del Anexo al Acuerdo,

la falta de especificación clara sobre los fines para los cuales se retienen los datos, lo que no permite realizar un juicio adecuado de proporcionalidad en relación al tiempo de retención establecido en el Acuerdo.[1034]

En cuanto a la transmisión a terceros, el Acuerdo autoriza al Servicio de Aduanas Australiano, a comunicar los datos del PNR, tanto dentro del Gobierno de Australia, como a terceros países. En el primer caso, se prevé que el Servicio de Aduanas Australiano podrá transferir los datos del PNR sólo a determinados departamentos y agencias del gobierno australiano cuando sean anónimos.[1035] Esta disposición es positiva, ya que protege el derecho a la intimidad de los pasajeros aéreos, para evitar su identificación y mantener su anonimato. En cuanto a la divulgación a los gobiernos de terceros países se refiere, el Acuerdo establece que las aduanas pueden decidir la transferencia de datos PNR a ciertas autoridades gubernamentales de terceros países en un análisis caso por caso.[1036] Esta norma no define claramente los criterios y los requisitos para admitir la difusión de los datos del PNR a terceros países, ni tampoco hace referencia al criterio de la necesidad de garantizar un adecuado nivel de protección por un tercer Estado. Esto podría dar lugar a abusos por parte del SSA, ya que estaría facultado para infringir el derecho a la protección de datos personales de los pasajeros.

No obstante lo anterior, existen varios aspectos positivos de este Acuerdo que vale la pena destacar. En primer lugar, establece un sistema acceso y rectificación de los datos en favor de las personas afectadas, con independencia de su nacionalidad o país de residencia.[1037] Por otra parte, es un sistema que contempla la protección del derecho a la privacidad de los pasajeros, que permite a las personas afectadas reclamar. Por último, establece una revisión periódica por las partes, que incluye "las garantías sobre protección de los datos y sobre seguridad de los datos, para garantizarse mutuamente la aplicación eficaz del Acuerdo."[1038] Sin embargo, como también se ha recordado por el Parlamento Europeo, el Acuerdo no prevé un plazo preciso para esta revisión. [1039]

[1034] En el mismo sentido véase la letra n) de la Recomendación del Parlamento Europeo, de 22 de octubre de 2008, destinada al Consejo sobre la celebración del Acuerdo entre la Unión Europea y Australia sobre el tratamiento y la transferencia de datos, generados en la Unión Europea, del registro de nombres de los pasajeros (PNR) por las compañías aéreas a los Servicios de Aduanas de Australia (2008/2187(INI)).
[1035] Cfr. párrafos 2-5 del Anexo al Acuerdo UE-Australia sobre el PNR.
[1036] Ibídem., párrafo 6.
[1037] Artículo 7 del Acuerdo UE-Australia sobre el PNR.
[1038] Ibídem., artículo 9.
[1039] Letra l) de la Recomendación del Parlamento Europeo de 22 de octubre 2008.

4.4. Análisis de la propuesta de 2007 para la creación de un PNR europeo

En noviembre de 2007, el Consejo presentó una Propuesta de Decisión Marco sobre utilización de datos del PNR con fines represivos (en adelante, "la Propuesta").[1040] Esta tiene por objeto armonizar las disposiciones de los Estados Miembros relativas a la obligación de las compañías aéreas, que ofrecen vuelos hacia o desde la Unión Europea, de transmitir los datos PNR a las autoridades competentes con el fin de prevenir atentados terroristas, la delincuencia organizada, y luchar contra ellos.[1041]

Es esencial establecer criterios generales que armonicen la legislación de los Estados Miembros, ya que actualmente en la UE, el Reino Unido dispone de un sistema PNR en funcionamiento, y otros Estados Miembros han adoptado la legislación pertinente o están probando la utilización de datos PNR.[1042] En este sentido, la iniciativa que comentamos es bienvenida, no obstante, se ha criticado la propuesta por contener disposiciones muy similares al Acuerdo UE-EE.UU. sobre PNR, y por pretender un uso extensivo de estos datos, ya que dichas medidas se aplicarían a todos los pasajeros con la finalidad de "realizar evaluaciones del riesgo que presentan las personas, obtener información analítica y establecer relaciones entre personas conocidas y desconocidas", independientemente de si "se estén investigando o no".[1043]

La propuesta hace referencia a las disposiciones previstas en la Directiva 2004/82/CE sobre la obligación de los transportistas de comunicar los datos de la API a las autoridades competentes.[1044] De acuerdo con la propuesta, la recogida de datos de los PNR es una herramienta mucho más eficaz en la lucha contra el terrorismo internacional que la recogida de datos de la API, ya que permitiría con una mayor

[1040] Propuesta de Decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros (*Passenger Name Record* - PNR) con fines represivos. COM (2007) 654 final, de fecha 6.11.2007.
[1041] Ibídem., p. 7.
[1042] Comunicación de la Comisión COM(2010) 492 final, p. 3
[1043] Cfr. Dictamen del Supervisor Europeo de Protección de Datos, acerca de la propuesta de Decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros (Passenger Name Record — PNR) con fines represivos, publicado en el Diario Oficial de la UE nº C 110 de 1.5.2008, p. 1/15
[1044] Propuesta de Decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros (Passenger Name Record - PNR) con fines represivos. COM(2007) 654 final, de fecha 6.11.2007, p. 3.

anticipación "proceder a evaluaciones del riesgo que puedan entrañar las personas, obtener información y establecer vínculos entre personas conocidas y desconocidas".[1045] Las autoridades comunitarias responsables de la protección de datos consideran que la forma en que la propuesta está actualmente redactada no sólo es desproporcionada, sino que también puede violar principios fundamentales de normas reconocidas en materia de protección de datos recogidas en el artículo 8 del Convenio Europeo sobre Derechos Humanos y del Convenio 108 del Consejo de Europa.[1046]

En cuanto a las autoridades encargadas del tratamiento (recogida, análisis evaluación y transmisión de los datos del PNR) la propuesta establece un sistema descentralizado, en virtud del cual las compañías aéreas están obligadas a la transferencia de datos PNR a las Unidades de Información sobre Pasajeros (UIP), que serán designadas por cada Estado miembro.[1047] Este sistema descentralizado, desde un punto de vista de la protección de datos, podría resultar ser un planteamiento mejor, pero también ocasionar niveles de protección de datos y sistemas técnicos divergentes en los distintos Estados Miembros.[1048] Cada Estado miembro debe elaborar una lista indicando cuales son las autoridades competentes facultadas para recibir datos PNR de las UIP y tratar dichos datos.[1049] Sólo estas autoridades podrán ser las responsables de prevenir o combatir los delitos de terrorismo y la delincuencia organizada.[1050]

Respecto del tipo de información que se transfieren, la propuesta establece diecinueve elementos, que incluye toda la información necesaria para el tratamiento y control de las reservas por parte de las compañías aéreas y los datos del sistema API. En caso de menores de 18 años que no viajen acompañados, se suman seis datos adicionales sobre identificación del menor, los acompañantes en el aeropuerto de origen

[1045] Ídem.
[1046] Dictamen conjunto del Grupo de Trabajo del artículo 29 y del Grupo de Trabajo Policía y Justicia, sobre la propuesta de Decisión marco del Consejo relativa al uso del registro de nombres de los pasajeros («Passenger Name Record» - PNR) a efectos de la aplicación de la ley, presentado por la Comisión el 6 de noviembre de 2007.
[1047] Artículo 3 de la propuesta de Decisión Marco, pp. 14-15.
[1048] Dictamen conjunto del Grupo de Trabajo del artículo 29 y del Grupo de Trabajo Policía y Justicia, sobre la propuesta de Decisión Marco del Consejo relativa al uso del registro de nombres de los pasajeros («Passenger Name Record» - PNR) a efectos de la aplicación de la ley, presentado por la Comisión el 6 de noviembre de 2007, p. 7
[1049] Artículo 4.1 de la Propuesta de Decisión Marco.
[1050] Ibídem., artículo 4.2

y destino, y del agente en el lugar de salida y entrada.[1051] El número y la naturaleza de los datos del PNR que se transfieren, de acuerdo con la propuesta, son prácticamente los mismos que los datos señalados en el Acuerdo UE y los Estados Unidos de Norteamérica (2007), por lo que se han hecho extensivas las críticas formuladas a éste, en el sentido de que la transferencia de tal número de elementos da a las autoridades competentes de control poderes amplios de vigilancia sobre la vida privada de las personas, sin que se haya explicado y probado hasta ahora por qué son necesarios tantos elementos. [1052]

Sobre el método de transferencia de la información, la propuesta plantea como regla general el método *push*, no obstante, cuando la compañía aérea no posea la arquitectura técnica necesaria para utilizar este método, deberán permitir que la UIP, o el intermediario designado con arreglo al artículo 6, extraiga los datos de sus bases con el método *pull*. Las Autoridades de Protección de Datos de la UE están de acuerdo con la implantación de este sistema, pero advierten que "no está claro cómo podrá cada UIP tratar con todas las compañías establecidas fuera de la UE que todavía no disponen de medios técnicos para transferir (*push)* los datos, con lo que hay que extraerlos (*pull)* a partir de muchos sistemas distintos". También plantean sus dudas sobre "cómo obtener datos de compañías que no operan con sistemas de reserva electrónicos". Por último, señalan que "habrá que resolver también cuestiones de aplicación de la ley, cuando haya que extraer los datos y la compañía aérea de un tercer país no acepte que la UIP de un Estado miembro acceda a dichos datos".[1053]

Respecto de las transferencias de datos del PNR hacia terceros países, la propuesta las permite bajo una doble condición: por una parte, que las autoridades del tercer país solamente utilicen los datos a efectos de prevención y lucha contra delitos de terrorismo y delincuencia organizada, y por otra, que no transfieran los datos a otro tercer país sin el consentimiento expreso del Estado miembro donde se originaron los

[1051] Anexo I de la Propuesta de Decisión Marco, pp. 26-27.
[1052] Dictamen conjunto del Grupo de Trabajo del artículo 29 y del Grupo de Trabajo Policía y Justicia, *supra nota* 180, p. 10; y Dictamen del Supervisor Europeo de Protección de Datos, acerca de la propuesta de Decisión Marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros (Passenger Name Record — PNR) con fines represivos, publicado en el Diario Oficial de la UE nº C 110 de 1.5.2008, p. 12.
[1053] Dictamen conjunto del Grupo de Trabajo del artículo 29 y del Grupo de Trabajo Policía y Justicia, p. 8.

datos.[1054] Además, establece como garantías que este tipo de transferencias está sujeto a la Decisión Marco relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, y que la transferencia debe cumplir las disposiciones de la legislación nacional del Estado miembro de que se trate y las de cualesquiera acuerdos internacionales aplicables.[1055] Tanto las Autoridades de Protección de Datos europeas, como el SEPD han criticado la propuesta en materia de transferencias internacionales de datos a terceros países, entre otros motivos, por no especificar las condiciones bajo las cuales un Estado miembro puede expresar su consentimiento y no hacer referencia a la necesidad de que el tercer país debe asegurar un nivel adecuado de protección.[1056]

Respecto del periodo de conservación de los datos, la propuesta establece en su artículo 9 que se mantengan en una base de datos en la Unidad de Información sobre Pasajeros durante un período de cinco años, luego del cual, los datos se mantendrán por otro período adicional de ocho años, para ser utilizados en caso de circunstancias excepcionales en respuesta a una amenaza o riesgo específico y real relacionado con la prevención y lucha contra los delitos de terrorismo y la delincuencia organizada. Este plazo de trece años, muy cercano al término de quince años previsto en el Acuerdo UE-EE.UU, nos parece excesivo y desproporcionado, afectando sensiblemente el derecho a la intimidad de las personas.

Evaluando la Propuesta en su conjunto, queremos destacar positivamente algunos aspectos de la misma. En primer lugar, es un avance el intento de armonizar la legislación de los Estados Miembros de la UE relativas a la transferencia de datos PNR, ya que por esta vía se refuerza la certeza de la ley y se garantiza el Estado de Derecho. También es destacable la especificación de los fines para los cuales se utilizarán los datos del PNR, limitándolos a la prevención y lucha contra el terrorismo y la delincuencia organizada. La Propuesta establece una preferencia por un método *push* de transmisión de los datos, que brinda la posibilidad de un mayor control de los mismos.

[1054] Artículo 8 de la Propuesta de Decisión marco, p. 19
[1055] Ídem.
[1056] Dictamen conjunto del Grupo de Trabajo del artículo 29 y del Grupo de Trabajo Policía y Justicia, p. 9; y Dictamen conjunto del Grupo de Trabajo del artículo 29 y del Grupo de Trabajo Policía y Justicia, sobre la propuesta de Decisión marco del Consejo relativa al uso del registro de nombres de los pasajeros (*«Passenger Name Record»* - PNR) a efectos de la aplicación de la ley, presentado por la Comisión el 6 de noviembre de 2007, pp. 10-11.

Por último, queremos destacar la exclusión de los datos sensibles dentro de los datos del PNR a transmitir.

No obstante, también se deben señalar muchos aspectos negativos de la Propuesta, que se resumen en las dudas sobre la eficacia, proporcionalidad y necesidad de las medidas previstas; la cantidad excesiva de elementos de datos a tratar, enumerados en el anexo I; la desproporción en el período de conservación de los datos (trece años); y la vulneración ciertos derechos fundamentales, en particular el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea.

CONCLUSIONES

1. El avance progresivo, exponencial e irreversible de las tecnologías de la información y las comunicaciones ha traído grandes progresos para la humanidad. No obstante, ello también ha originado ciertos peligros derivados del uso disfuncional de los medios tecnológicos, que han puesto en riesgo el ejercicio de algunos derechos y libertades fundamentales. En efecto, los avances técnicos permiten en la actualidad almacenar, relacionar y transferir un número casi ilimitados de datos, incluyendo por cierto, todo tipo de datos personales para ser utilizados en diversas actividades por entes públicos y privados. Más aún, hemos llegado al punto en que, mediante la combinación de diversas fuentes de información, se puede tener una idea clara sobre aspectos relevantes del comportamiento vital de una persona, o incluso obtener una imagen representativa de su personalidad.

2. Por otra parte, producto de la amenaza terrorista, en los últimos quince años han aumentado e intensificado las transferencias de datos personales entre las fuerzas y cuerpos de seguridad de los Estados miembros de la Unión Europea, así como entre ésta y terceros Estados. Bajo el argumento de una mayor seguridad de las personas, se tratan (recolectan, analizan, transfieren o ponen a disposición a favor de otros Estados) una cantidad exorbitante de datos de carácter personal con la finalidad de prevenir y reprimir la comisión de éste tipo de ilícitos u otras formas graves de delincuencia transnacional. Lo anterior supone la necesidad de conciliar, por una parte, la operativización del *principio de disponibilidad*, permitiendo un intercambio fluido de información por parte de las policías, y por otra, el debido respeto los derechos y libertades fundamentales de las personas, incluidos los de los potenciales y reales delincuentes. Lo anterior no es baladí, ya que si se otorga un poder ilimitado al Estado para el manejo de la información personal de sus ciudadanos en aras de la seguridad, se puede llegar fácilmente a un Estado casi totalitario, con característica orwelianas, donde los ciudadanos, consciente o inconscientemente, forzada o voluntariamente, prestan su consentimiento para el tratamiento de su información personal, en la medida que el Estado le garantice una mayor *sensación* de seguridad.

3. Frente a esta realidad, se ha ido construyendo un derecho de nuevo cuño, vinculado esencialmente al desarrollo tecnológico —fotografía instantánea, informática, internet, entre otros—. Desde las primeras reflexiones doctrinarias realizadas a fines del siglo XIX en Estados Unidos de Norteamérica, primero con el juez Cooley y luego con el decisivo trabajo de Warren y Brandeis, se plantea el nacimiento de un nuevo derecho, cuyo soporte es la dignidad de la persona y el libre desarrollo de su personalidad. Estas ideas serán reformuladas ante el surgimiento y desarrollo de la informática, planteando la necesidad de resguardar la autodeterminación de las personas y la información personal de las mismas, con la finalidad de que el individuo disponga de un control real sobre su información personal. Con la irrupción de Internet, el paradigma de la autodeterminación informativa carece de sentido sin una norma pública que establezca un estándar mínimo a cumplir.

4. En Europa, por su parte, se generaron diversas posturas respecto de cómo abordar el tema de la protección de los datos personales frente al fenómeno informático. Así, algunos propugnaron una recepción amplia de la *privacy* norteamericana, tanto en su denominación como en su contenido. Otros pretendieron establecer un cierto paralelismo entre la *privacy* y el derecho a la intimidad o la vida privada, tratando de ampliar el contenido de éstas a fin de dar cobertura a la nueva realidad que se presentaba; y por último, se encuentran aquellos que proponían la construcción de un nuevo derecho fundamental con identidad propia, a fin de tutelar adecuadamente a las personas frente a los peligros generados por parte de la informática y las TIC.

En definitiva, la configuración del derecho fundamental a la protección de datos personales, como un derecho autónomo e independiente de otros institutos jurídicos afines, es el fruto de un largo proceso evolutivo, donde la doctrina, legislación y jurisprudencia (nacional y europea) han jugado un papel central.

5. Los retos que propone el derecho fundamental a la protección de los datos personales exceden las tradicionales fronteras de los Estados e incluso de zonas geográfica completas, y se instala como un *problema global* en un mundo interdependiente, y que por tanto, demanda soluciones del mismo alcance. En esta línea, las directrices y recomendaciones internacionales (ONU, APEC, OCDE, entre otros) han jugado un papel central en el proceso de homologación de los principios, derecho y obligaciones mínimas a respetar en la materia. No obstante, la mayoría de estos instrumentos carecen

de fuerza jurídica vinculante, y sólo constituyen una referencia para los Estados. Por ello, es urgente avanzar hacia un **convenio jurídico universal y vinculante**, tecnológicamente neutral y certificable en materia de protección de datos personales y privacidad. En este sentido, la Resolución de Madrid que consagra unos estándares internacionales sobre privacidad y protección de datos, es un primer paso para alcanzar dicho fin.

6. El marco normativo aplicable a la protección de datos personales en el ámbito de la prevención y represión penal en Europa, está dado por la conjugación de normas supranacionales provenientes tanto del Consejo de Europa como de aquellas emanadas de las diversas fases del proceso de consolidación de la Unión Europea. Además, debe sumarse a ello, las normas de cada Estado, e incluso, normas locales en el caso de los Estados federados o plurinacionales. La interrelación de estas normas de diversos niveles ha permitido que Europa se convierta en uno de los ámbitos político geográfico donde el derecho fundamental a la protección de datos ha tenido mayor dinamismo. Desde la labor pionera desarrollada por el Consejo de Europa a partir de la década de los sesentas, hasta la consagración definitiva de la protección de datos personales como derecho fundamental autónomo en el artículo 8º de la Carta Europea de Derechos Fundamentales, a principios del presente siglo, se puede ver la evolución y adaptación de este derecho en la jurisprudencia, doctrina y legislación Europea y de los Estados miembros.

7. En el ámbito normativo del Consejo de Europa, encontramos en primer lugar el CEDH de 1950. Dicho instrumento no tiene reconocido en su texto a la protección de datos personales como un derecho fundamental autónomo. No obstante, el TEDH, mediante una interpretación extensiva del derecho a la «vida privada», reconocido en el artículo 8, ha incluido dentro del ámbito o campo de protección la recogida, almacenamiento o difusión de datos personales de cualquier tipo. De esta forma, los datos personales forman parte de la «esfera privada» y, en consecuencia, del ámbito protegido por el derecho a la vida privada reconocido en el artículo 8 del CEDH.

En 1981 el Consejo de Europa aprobó un instrumento jurídico específico destinado a garantizar a las personas físicas el respeto de su derecho a la vida privada con respecto al tratamiento automatizado de los datos de carácter personal: El Convenio n° 108. En él se establece un estándar mínimo de protección, aplicable tanto al ámbito público como

privado, y ampliable por las legislaciones nacionales. Este estándar mínimo conlleva una serie de derechos instrumentales y principios básicos que los Estados partes deben tener en cuenta a la hora de adoptar en su derecho interno las medidas que hagan efectiva la protección de los datos personales. De esta forma, se logra el objetivo final del Convenio de resguardar los datos personales, como una forma de cautelar el derecho a la vida privada, estableciendo principios esenciales, derechos y garantías mínimas para ello, con el fin de liberalizar la circulación de la información (datos) entre los Estados miembros.

Con la Recomendación 87 (15), el Consejo de Europa reelabora los principios contenidos en el Convenio 108 para adecuarlo a las particularidades del tratamiento de datos personales por parte de la policía. Junto con realzar la utilidad del tratamiento de datos personales para la función policial, la Recomendación advierte sobre los peligros que dicha técnica puede tener para los derechos de las personas, proponiendo equilibrar los intereses en juego. Para ello, se elabora esta especie de guía de principios, derechos y obligaciones a tener en consideración por parte del derecho interno de los Estados miembros al momento de regular el tratamiento de datos personales en la práctica policial.

Si bien la Recomendación no es obligatoria para los Estados miembros, su impacto es indiscutible, ya que ha sido considerada por todos los instrumentos normativos elaborados por la Unión Europa referido al tema específico del tratamiento de datos con fines de represión y prevención penal como uno de los elementos a considerar al momento de determinar el nivel mínimo de protección que se debe dar a los interesados. Ello se debe en gran medida, en una primera etapa, a la falta de regulación sobre la materia en la Unión Europea, y luego, una vez aprobada la Decisión Marco 2008/977/JAI, al limitado ámbito de aplicación de la misma, lo que ha llevado a considerar a la Recomendación (87) 15 como un «**estándar de facto**» para la protección de datos en los tratamientos de los mismos llevados a cabo con finalidad de investigación policial en el ámbito europeo. Así, por ejemplo, se ha incorporado como uno de los elementos a considerar a la hora de determinar el nivel mínimo de protección en diversos convenios y decisiones de la UE, tales como Schengen, Europol, Sistema de Información Aduanera o Eurojust. Más aún, su influencia pervive hasta la actualidad, ya que la nueva Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales

con fines de prevención y represión penal, COM(2012) 10 final, hace mención en su exposición de motivos a esta Resolución del Consejo de Europa.

8. La normativa de protección de datos en la Unión Europea tiene en principio un marco bien definido, configurado por tratados internacionales, directivas y la correspondiente normativa interna desarrollada por los Estados miembros. Ello es así, al menos, por lo que respecta al antiguo primer pilar comunitario, pero dicha normativa se encuentra actualmente ante un reto específico: su definición y asentamiento en el marco del antiguo tercer pilar comunitario, sin olvidar el encaje de dicha normativa ante los cambios que trae el Tratado de Lisboa.

Si bien, con el Tratado de Lisboa se produce una supresión formal de la estructura de pilares de la Unión y comunitariza el área de Libertad, Seguridad y Justicia, ello no implica que la Directiva comunitaria 95/46/CE sea aplicable al ámbito policial, ya que sigue vigente la exclusión que realiza el artículo 3.2.1 de la Directiva y la declaración anexa al Tratado sobre el artículo 16. Por otra parte, el hecho que la Decisión Marco 2008/977/JAI haya entrado en vigencia antes del Tratado de Lisboa, fosilizó cualquier modificación sobre su ámbito de aplicación hasta que se apruebe la nueva iniciativa legislativa que la reemplazará.

Asimismo, el Tribunal de Justicia de la UE será competente en éste ámbito en relación a instrumentos legales posteriores al tratado o modificados tras el Tratado, pero no durante los primeros cinco años en relación a actos legislativos anteriores al Tratado (artículo 10 del Protocolo). Por último, el cambio en la ubicación sistemática de la regulación de la protección de datos en el Tratado de Lisboa, que pasa a regularse en el artículo 16 del TFUE, incluyendo la cooperación judicial y policial en materia penal, a diferencia de la que ocurría antes, donde el artículo 286 TUE limitaba su aplicación al ámbito comunitario, es una clara manifestación de la importancia que ha cobrado esta materia en el concierto europeo.

En el ámbito específico de la cooperación policial, el Tratado de Funcionamiento de la Unión Europea busca la colaboración entre los servicios de policía, de aduanas y otros servicios con funciones coercitivas. Para ello se contempla la posibilidad de que, por vía del procedimiento legislativo ordinario, se adopten disposiciones que tengan relación con el tratamiento de datos personales (artículo 87.2 TFUE). No obstante, en caso de no lograse un acuerdo por ésta vía, se establece la posibilidad de una

«cooperación reforzada» sobre éstas materias, con la única exclusión de aquellos actos que constituyan un desarrollo del Acuerdo Schengen.

9. A diferencia del CEDH, en que sólo se reconoce el derecho a la vida privada, la Carta de Derechos Fundamentales de la Unión Europea va a reconocer, por una parte, el derecho al respeto a la vida privada y familiar (artículo 7), y por otro, el derecho a la protección de datos personales (artículo 8), consagrando ambos derechos de forma independiente y autónoma. Con la finalidad de que la CDFUE fuera jurídicamente vinculante, los Presidentes del Parlamento, del Consejo y de la Comisión Europea firmaron y volvieron a proclamar solemnemente la Carta en 2007. Si bien la CDFUE no forma parte del texto del Tratado de Lisboa, por remisión del actual artículo 6 del Tratado de la Unión Europea, se hace vinculante para todos los Estados con el mismo valor jurídico que los Tratados (TUE y TFUE).

10. En el ámbito específico de la protección de datos personales, se ha dictado varias Directivas, Reglamentos y Decisiones que regulan o establecen parámetros comunes a seguir en ciertas áreas específicas que afectan la protección de los datos personales. Todos estos instrumentos forman parte de lo que se denomina Derecho derivado de la Unión o actos legislativos de la Unión.

La Directiva 95/46/CE es una pieza fundamental dentro del derecho derivado europeo en materia de protección de los datos personales, ya que establece el marco general y común a aplicar en materia de protección de datos personales en el antiguo primer pilar comunitario de la Unión Europea. La Directiva, bajo la antigua lógica de división de pilares comunitarios, estableció una serie de materias que quedan excluidas de su campo de aplicación material. Por tanto, sus normas no se aplican al tratamiento de datos personales que se efectúen en el ejercicio de actividades no comprendidas en el ámbito de aplicación del derecho comunitario —antiguo primer pilar comunitario—, como tampoco a las materias previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea —antiguo segundo y tercer pilar comunitario— y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del mismo), y las actividades del Estado en materia penal. En consecuencia, **la Directiva 95/46 excluye de su ámbito de aplicación los datos policiales**.

Con la finalidad de dar cumplimiento a lo dispuesto en el artículo 16.2 del TFUE, la Comisión ha propuesto una serie de importantes reformas a las normas de la Unión Europea en materia de protección de los datos personales, que pretenden actualizar y modernizar los principios consagrados en la Directiva de 1995, para garantizar el derecho a la protección de los datos personales en el futuro.

Con posterioridad a la Directiva 95/46/CE se han dictado una serie de Directivas sectoriales. Una de las más cuestionadas fue la Directiva 2006/24/CE, de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones con fines de prevención y represión penal. En una priemra etapa se cuestionó la utilización del artículo 95 del TCE como base jurídica para la misma, por ser incongruente con su finalidad: garantizar la disponibilidad de los datos tratados por los proveedores de servicios de comunicaciones electrónicas con fines de investigación, detección y enjuiciamiento de delitos graves, aspecto propio del antiguo tercer pilar comunitario. Ello llevó a Irlanda en julio de 2006 a iniciar un proceso ante el TJCE con el fin de lograr la anulación de la Directiva 2006/24/CE, pero dicha acción fue desestimada por el tribunal al considerar que la Directiva en cuestión se justificaba en la necesidad de una norma armonizadora de las legislaciones nacionales de los Estados Miembros sobre conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas, actividad que consideró como relevante y de impacto directo en el mercado interior. Esta postura del TJUE, cambió con el reciente fallo de 8 de abril de 2014, que invalidad la Directiva por la injerencia desproporcionada que significa en relación a los derechos garantizados en el artículo 7 (vida privada) y 8 (protección de datos) del CDFUE. Esta situación evidencia, por una parte, la dificultad que revestía encuadrar algunas normas europeas en alguno de los extintos pilares comunitarios, atendido que varias de las Directivas y Reglamentos excedían de lo estrictamente necesario para el desarrollo del mercado interior, y pasaban a regular materias propias de la prevención y represión penal del antiguo tercer pilar comunitario. Por otra parte, y no menos importante, deja clara la tendencia cada vez mayor de las autoridades públicas europeas de exigir a compañías privadas la entrega o el acceso a los datos personales que consten en sus registros, todo ello bajo el amplio concepto del resguardo de la seguridad nacional.

Otro instrumento jurídico general relevante para la protección de datos personales es el Reglamento 45/2001 de 18 de diciembre de 2000 relativo al tratamiento de datos

personales por las instituciones y los organismos comunitarios, y a la libre circulación de estos datos. Al igual que las Directivas analizadas precedentemente, su finalidad es dual. Por una parte, persiguen que las instituciones y organismos comunitarios garanticen la protección efectiva de los derechos y las libertades fundamentales de las personas físicas y, en particular, su derecho a la intimidad en lo que respecta al tratamiento de los datos personales. Por otra parte, buscan que dichos organismos e instituciones no limiten ni prohíban la libre circulación de datos personales entre ellos, o entre ellos y destinatarios de los Estados Miembros. Para supervisar el cumplimiento de sus disposiciones se crea la figura del Supervisor Europeo de Protección de Datos, órgano que ha devenido en esencial para la debida cautela del derecho fundamental a la protección de datos en todos los ámbitos del derecho europeo y que, con posterioridad al Tratado de Lisboa, ha ido adquiriendo cada vez más protagonismo y responsabilidad en su labor.

Éste Reglamento se aplica exclusivamente al tratamiento de datos personales por parte de todas las instituciones y organismos comunitarios en el ámbito de aplicación del derecho comunitario, esto es, del antiguo primer pilar comunitario. Por tanto, en principio, toda la actividad realizada por organismos públicos europeos encargados de la prevención y represión penal estarían excluidos del ámbito de aplicación del Reglamento. No obstante, si se analizan las disposiciones vigentes de Europol, Eurojust, así como de los grandes sistemas de información que actualmente se utilizan para la prevención de ilícitos transnacionales a nivel europeo (SIS, VIS, EURODAC, entre otros), todas ellas remiten al Reglamento 45/2001 como norma supletoria aplicable al tratamiento de datos personales, y al Supervisor Europeo de Protección de datos como autoridad de control.

11. El actual marco normativo europeo sobre protección de datos en el ámbito específico de la cooperación policial penal carece de un desarrollo coordinado y homogéneo, y se presenta como un **conjunto atomizado por áreas temáticas**. Ello se debe, en primer lugar, a la inexistencia, hasta hace poco, de una norma de carácter general destinada a regular la materia, rol que debió cumplir la Decisión Marco 2008/977/JAI, pero que, atendido su limitado ámbito de aplicación, no cumplió. En segundo lugar, ha influido el hecho de que cada norma desarrollada antes de la Decisión Marco 2008, referida al tratamiento de datos personales con fines de prevención y represión penal o con directa incidencia en él, consagró disposiciones particulares sobre protección de datos. En su

mayoría, dichas disposiciones, remitían al derecho interno de cada Estado como forma o mecanismo de resguardar los derechos de los titulares de los datos, generando una disparidad de criterios de un Estado a otro.

A lo anterior se suman algunas iniciativas llevadas a cabo en el seno de la Unión Europea, como el desarrollo del Programa de La Haya, la incorporación de los aspectos esenciales del Tratado de Prüm en el ordenamiento jurídico de la Unión Europea a través de la Decisión 2008/615/JAI del Consejo de 23 de junio, o el desarrollo del llamado PNR europeo a través de la propuesta del Consejo sobre utilización de datos del registro de nombres de los pasajeros con fines represivos.

12. La Unión Europea dictó la Decisión Marco 2008/977/JAI precisamente para regular la protección de datos personales en el ámbito de la cooperación policial y judicial en materia penal (antiguo tercer pilar comunitario). No obstante, atendido su limitado ámbito de aplicación, dicha norma no puede ser calificada como una norma general y supletoria para el tratamiento de datos con fines policiales. Por la misma razón, no se le puede equiparar con la función que cumple la Directiva 95/46/CE en el antiguo primer pilar comunitario. La Decisión Marco excluye de su ámbito de aplicación el tratamiento nacional o doméstico, así como los tratamientos de datos personales realizados por Europol, Eurojust y los sistemas de información de visados y Schengen.

El hecho que la Decisión Marco 2008/977/JAI solo se aplique al tratamiento transfronterizo de datos y no a las actividades de tratamiento por parte de las autoridades policiales y judiciales a nivel puramente nacional, puede crear dificultades. En efecto, dada la naturaleza de éste tipo de tratamiento, las autoridades competentes no siempre son capaces de distinguir entre el tratamiento meramente nacional y el transfronterizo, o de prever que determinados datos personales pueden convertirse en objeto de un intercambio transfronterizo en una fase posterior. Además, por su naturaleza y contenido, la Decisión Marco deja un amplio margen de maniobra a los Estados miembros para transponer sus disposiciones de Derecho interno. Ello abre la posibilidad de un doble régimen en el tratamiento de este tipo de datos: uno interno o doméstico, y otro para los supuestos contemplados en la Decisión Marco. Además, no contiene ningún mecanismo o grupo consultivo similar al Grupo del artículo 29 que sustente una interpretación común de sus disposiciones, ni establece competencias de ejecución de la Comisión a fin de garantizar un enfoque común en su aplicación.

La Decisión Marco 2008/977/JAI tampoco afecta el tratamiento de datos personales realizado por la Oficina Europea de Policía (Europol), por la Unidad Europea de Cooperación Judicial (Eurojust), el Sistema de Información de Schengen (SIS) y el Sistema de Información Aduanero (SIA), ni en general, a los que permiten a las autoridades acceder directamente a determinados sistemas de datos de otros Estados miembros, y que tengan un objeto diferente al señalado en esta DM 2008/977/JAI. Tampoco se aplica la Decisión Marco a las disposiciones de protección de datos que rigen la transferencia automatizada de perfiles de ADN, datos dactiloscópicos y datos de los registros nacionales de matriculación de vehículos, en virtud de la Decisión 2008/615/JAI del Consejo. Asimismo, la Decisión Marco excluye específicamente de su ámbito de aplicación las materias propias del antiguo segundo pilar comunitario, estos es, las vinculadas a los intereses esenciales de seguridad del Estado y a las actividades específicas de inteligencia en éste sector.

Estas exclusiones se justifican por el legislador comunitario en un supuesto **principio de especialidad** de dichas normas. Se señala que estos sistemas excluidos contienen un conjunto completo y coherente de normas que abarcan todos los aspectos correspondientes a la protección de los datos (principios de calidad, normas sobre seguridad de los datos, reglamentación de los derechos y protecciones de los interesados, organización del control y responsabilidad), que reglamentan estos asuntos con más detalle incluso que la Decisión Marco.

Para nosotros, lo anterior sólo se justifica en la medida que las previsiones sobre protección de datos contenidas en las citadas bases de datos, contengan efectivamente disposiciones que garanticen un nivel igual o mayor de protección que la Decisión Marco, lo que obligatoriamente nos obliga a realizar una comparación del nivel de protección de cada uno de ellos.

13. La proliferación de normas especiales en materia de tratamiento de datos personales en áreas vinculadas a la prevención y represión penal, se produce por la ausencia de una norma general de la Unión Europea en la materia. Al respecto cabe recordar que 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, no se aplica al tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del derecho comunitario, como son las contempladas en el título VI del

Tratado de la Unión Europea, ni en ningún caso a las operaciones de tratamiento de datos relacionadas con la seguridad pública, la defensa, la seguridad del Estado o las actuaciones de este en materia penal.

Ante la ausencia de una norma de carácter general, que establezca los principios y obligaciones básicas en el tratamiento de datos con fines preventivos y represivos en materia penal, la Unión Europea dictó normas para regular **ámbitos concretos de la actuación policial y judicial**, incorporando disposiciones sobre protección de datos en regulaciones específicas. Así ocurre, por ejemplo, con el tratamiento de datos personales realizado por la Oficina Europea de Policía (Europol), por la Unidad Europea de Cooperación Judicial (Eurojust), el Sistema de Información de Schengen (SIS) y el Sistema de Información Aduanero (SIA), y la Decisión marco 2008/615/JAI, que incorporó Prüm al ordenamiento jurídico europeo.

Todas estas instituciones, bases de datos y cuerpos normativos, tienen normas *específicas* sobre protección de datos personales, pero también todas ellas, se remiten al conjunto de disposiciones del Consejo de Europa, al momento de determinar los mínimos a cumplir por cada Estado para poder transferir datos de carácter personal. De ésta forma el bloque normativo constituido por el Convenio 108 de 1981, su Protocolo adicional de 2001 y la Recomendación (87) 15, todas del Consejo de Europa, pasaron a constituir el **estándar mínimo de protección** a respetar por parte de los Estados y organismo comunitarios en el tratamiento de los datos personales, en el ámbito específico de la cooperación policial y judicial en materia penal.

14. La propuesta de Directiva del Parlamento Europeo y del Consejo, COM(2012) 10 final, de 25 de enero de 2012, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos, responde, por una parte, a la necesidad de adecuar el marco jurídico de la protección de datos personales en la UE a lo prescrito por el Tratado de Lisboa y, por otra, a tratar de corregir importantes falencias que posee la Decisión Marco 2008/977/JAI.

La propuesta de Directiva, que pretende sustituir y derogar la Decisión Marco, se presenta como un intento de **homogenizar** los niveles de protección que se brindan en los otros ámbitos del derecho de la Unión (particularmente el antiguo primer pilar), pero teniendo en consideración las necesidades específicas en el ámbito de la cooperación

policial y judicial, lo que en la práctica se traduce en una serie de limitaciones y excepciones al ejercicio de los derechos de los titulares de los datos.

La propuesta de Directiva se hace cargo de algunas de las principales **críticas** que se han formulado a la Decisión Marco 2008/977/JAI. Así, ella se aplica tanto al tratamiento transfronterizo de datos (dentro y fuera de la Unión), como a las actividades de tratamiento realizadas por parte de las autoridades policiales y judiciales a nivel puramente nacional (tratamiento doméstico). También se establece un grupo consultivo similar al Grupo del artículo 29 que sustente una interpretación común de sus disposiciones, y da competencias de ejecución de la Comisión a fin de garantizar un enfoque común en su aplicación. La inclusión del «tratamiento nacional» (doméstico), no está explícitamente señalado en el articulado de la Propuesta, pero se deduce del conjunto de sus disposiciones, así como también de su exposición de motivos y considerandos.

Este punto constituye un avance en relación a la Decisión Marco 2008/977/JAI, la cual sólo tenía como ámbito de aplicación el tratamiento transfronterizo, pero es un **avance limitado** atendido al conjunto de restricción que se le colocan a la propuesta en cuanto a su extensión. En efecto, la propuesta excluye de su ámbito de aplicación los tratamientos realizados en el ejercicio de una actividad que no esté comprendida en el ámbito de aplicación del Derecho de la Unión, en especial en lo referido a la seguridad nacional, ni a las operaciones de tratamiento efectuadas por instituciones, órganos y organismos de la Unión, que están sujetas al Reglamento (CE) nº 45/2001 y otras normas específicas.

De esta forma, y reincidiendo uno de los aspectos criticados a la Decisión Marco 2008/977/JAI, la propuesta de Directiva excluiría de su ámbito de aplicación el tratamiento de datos personales realizado por la Oficina Europea de Policía (Europol), por la Unidad Europea de Cooperación Judicial (Eurojust), el Sistema de Información de Schengen (SIS) y el Sistema de Información Aduanero (SIA). Tampoco se aplicaría la propuesta de Directiva a las disposiciones de protección de datos que rigen la transferencia automatizada de perfiles de ADN, datos dactiloscópicos y datos de los registros nacionales de matriculación de vehículos, en virtud de la Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008 sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza. Asimismo, la propuesta de Directiva excluye

específicamente de su ámbito de aplicación las materias propias del antiguo segundo pilar comunitario.

15. Para determinar **el nivel mínimo de protección a garantizar**, proponemos realizar una ponderación del nivel que brinda cada uno de los instrumentos normativos que contienen normas específicas sobre tratamiento de datos en el ámbito policial y judicial, en relación a las garantías contenidas en la DM 2008/977/JAI o la propuesta que pretende derogarla y sucederla. Si de este examen de ponderación resulta que el cuerpo normativo particular disminuye los niveles de protección, se puede y debe recurrir a la aplicación supletoria de las disposiciones contenidas en los instrumentos normativos generales (Decisión Marco o propuesta de Directiva). Es más, creemos que en los futuros procesos de reforma de esta materia se debería considerar expresamente estos instrumentos generales con carácter supletorio y parámetro mínimo a respetar en el tratamiento de datos personales por parte de la policía y los tribunales.

Por último, no debemos olvidar que el Convenio 108 del Consejo de Europa sigue plenamente vigente y ha sido ratificado por todos los países miembros de la Unión. Dicho acuerdo supranacional se aplica tanto al ámbito público como al privado sin distinción, por tanto, también debe ser considerado al momento de determinar los estándares mínimos a respetar en la materia.

16. Un ámbito particularmente sensible al tratamiento de datos personales con fines de prevención y represión penal lo constituye la **lucha contra el terrorismo y otras formas graves de delincuencia transfronteriza**. La dimensión internacional de ambos fenómenos ha supuesto un reto para el Derecho, el cual aún no ha podido dar una respuesta adecuada, ni desde el Derecho internacional clásico, ni desde las legislaciones de los Estados, que resultan insuficientes para hacer frente con eficacia a la complejidad de una amenaza tal. Este reto es aún mayor si se piensa en las facilidades que brinda, por una parte, la globalización, y por otra, la libre circulación entre los Estados miembros de la Unión Europea. Se precisa, entonces, de instrumentos jurídicos adecuados para hacer frente a esta nueva realidad, pero no a cualquier precio, sino que respetando los valores de la democracia y Estado de derecho.

Uno de los instrumentos específicos dictados para combatir el terrorismo, la delincuencia transfronteriza y la migración ilegal, es la Decisión 2008/615/JAI del Consejo de 23 de junio de 2008 (en adelante, D2008/615/JAI), que incorpora los

aspectos esenciales de las disposiciones del Tratado de Prüm en el ordenamiento jurídico de la Unión Europea, con la finalidad de profundizar la cooperación transfronteriza entre los Estados miembros en éstas materias. Con el Convenio de Prüm se puso en práctica el «principio de disponibilidad» que busca simplificar el intercambio y acceso a información entre las autoridades de los Estados Miembros encargadas de la persecución y sanción penal.

Tanto el Tratado de Prüm como la Decisión 2008/615/JAI, contienen un conjunto de disposiciones relativas al tratamiento de datos personales. Para determinar el nivel de protección de datos, ambos instrumentos realizan una remisión o reenvío a las normas del Consejo de Europa. Se exige que cada Estado miembro garantice en su derecho interno un nivel de protección de datos equivalente, como mínimo, al que resulta del Convenio n° 108, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, el Protocolo adicional al Convenio de 8 de noviembre de 2001, y los principios de la Recomendación n° R(87) 15 del Consejo de Europa dirigida a regular la utilización de datos de carácter personal en el sector de la policía. El recurso al bloque normativo del Consejo de Europa fue necesario porque al momento de suscribir el Tratado de Prüm y aprobarse la Decisión Marco 2008/615/JAI, se carecía de una decisión marco sobre protección de datos en el denominado antiguo tercer pilar comunitario (cooperación policial y judicial). No obstante, la Decisión 2008/615/JAI supedita sus normas sobre protección de datos a una futura decisión marco que rija todos los ámbitos de la cooperación policial y judicial en materia penal, bajo la condición de que su nivel de protección de datos no sea inferior a la protección establecida por las normas del Consejo de Europa. Ahora bien, la Decisión Marco 2008/977/JAI, dictada con la finalidad de regir el tratamiento de datos personales en el ámbito de la cooperación policial y judicial, excluyó de su ámbito de aplicación a la Decisión 2008/615/JAI.

Esta situación se mantiene en la propuesta de Directiva que pretende derogar y reemplazar a la DM 2008/977/JAI. En consecuencia, el recurso a las disposiciones del Consejo de Europa para determinar el nivel mínimo a garantizar en el tratamiento de datos personales por parte de los órganos encargados de la prevención y represión penal, en los ámbitos de la lucha contra el terrorismo y la delincuencia transfronteriza regulados por la Decisión 2008/615/JAI, sigue plenamente vigente en la actualidad, mientras no se dicte una norma comunitaria que altere esta situación.

17. Para tener una visión completa del tratamiento de datos personales en el ámbito en ámbito de la cooperación judicial y policial europea, se debe incluir la normativa específica que regula el tratamiento de datos personales en Europol y Eurojust, así como de las agencias europeas encargadas de la coordinación de la prevención y represión penal paneuropea, incluyendo de los grandes sistemas de almacenamiento y gestión de información: Eurodac, Sistema de Información Schengen (SIS), el Sistema de Información de Visados (SIV), y el Sistema de Comparación de Huellas Dactilares (Eurodac), entre otros.

Es necesario determinar cuál es nivel de protección que se ofrece en estos sistemas y verificar si esta atomización normativa del antiguo tercer pilar comunitario, en lo que respecta al tratamiento de datos personales, se debe a una efectiva especificidad de sus disposiciones que justifique su exclusión del régimen general de protección de datos o, por el contrario, obedece a la intención no declarada de crear **ámbitos con regulación más laxa**, que tolere mayores restricciones a los derechos de los ciudadanos y menores limitaciones y controles judiciales y administrativos, bajo el supuesto genérico e indeterminado de protección de la seguridad.

La Oficina Europea de Policía (Europol) se constituyó originalmente con el fin de apoyar y reforzar la acción de las autoridades competentes de los Estados Miembros y su cooperación mutua en materia de prevención y lucha contra la delincuencia organizada, el terrorismo y otras formas de delitos graves que afecten a dos o más Estados Miembros. No obstante, diversas normas europeas, le han otorgando atribuciones en otras áreas. Con la entrada en vigor del Tratado de Lisboa el 1 de diciembre de 2009, las disposiciones sobre Europol han pasado a formar parte del Tratado de Funcionamiento de la Unión Europea (Título V – Espacio de Libertad, Seguridad y Justicia).

Europol facilita el intercambio de información entre las autoridades con funciones coercitivas de los Estados Miembros, y proporciona análisis criminales para ayudar a las fuerzas de policía nacionales a llevar a cabo investigaciones transfronterizas. Por tanto, el tratamiento de datos personales es inherente a la actividad que desarrolla Europol. El actual sistema establecido por la Decisión de 2009, crea y regula la gestión de un «sistema de información general» y «ficheros de trabajo de análisis». Los datos introducidos en estos sistemas pueden referirse tanto a personas involucradas en la comisión o que son sospechosas de planear algún delito, como también a información (datos) sobre testigos, víctimas, intermediarios, e incluso acompañantes del infractor.

Los datos personales tratados deben estar directamente relacionados con tales personas (nombre, nacionalidad, número de la seguridad social, entre otros) y con los delitos cometidos. Como se puede apreciar, el espectro de personas cuyos datos pueden ser tratados por esta mega base de datos es bastante amplio. Es por ello que el establecimiento de un sistema claro de *ejercicio de derechos* a favor de los interesados (titulares de los datos), y la imposición de *límites* a las potestades de Europol, se transforman en un imperativo si no queremos caer en una sociedad del control preventivo perenne.

Tanto la Decisión Europol de 2009, como la Propuesta de Reglamento de 2013, dedican un capítulo especial al tratamiento de datos personales. De esta forma se consolida un régimen jurídico particular para este tipo de tratamiento de datos. No obstante, la Propuesta de Reglamento introduce una modificación al respecto al establecer como **régimen supletorio**, en lo no regulado por ella, a los principios consagrados por el Reglamento 45/2001. Además, toma en consideración al Convenio nº 108, la Recomendación nº R (87) 24 del Consejo de Europa, y la Decisión Marco 2008/977/JAI del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial, incluyendo la Directiva que derogará y reemplazará a ésta última.

Otro organismo importante en el tratamiento de datos personales en el ámbito específico de la prevención y represión penal es Eurojust. Creada por la Decisión 2002/187/JAI del Consejo, tiene por finalidad reforzar la lucha contra las formas graves de delincuencia en la Unión Europea, mediante la coordinación entre las autoridades judiciales competentes de los Estados Miembros. En cumplimiento del mandato ordenado por el artículo 85 del TFUE, actualmente se encuentra en proceso de elaboración una propuesta de Reglamento que contempla todos estos elementos y ofrece un marco jurídico exclusivo y renovado para una nueva agencia de cooperación en materia de Justicia Penal. En lo que respecta al régimen aplicable al tratamiento de los datos personales, la propuesta de Reglamento realiza una triple distinción: entre tratamiento realizados por Eurojust en el marco de sus actividades; los datos transferidos desde los Estados Miembros a Eurojust; y, por último, respecto de las transferencias internacionales de datos desde Eurojust a organismos internacionales o terceros Estados. En este caso, al igual que la Propuesta de Europol, se establece como **régimen general y supletorio** aplicable al tratamiento de datos personales una norma de la Unión Europea, el Reglamento 45/2001. De ésta forma se pretende dar mayor

coherencia y uniformidad al sistema de protección de datos que se pretende construir el Postratado de Lisboa.

Otro órgano importante en el tratamiento de datos personales, con incidencia directa en la prevención y represión penal, es la Agencia Europea para la gestión de la cooperación operativa en las fronteras exteriores (Frontex). Creada en octubre de 2004 y modificada en varias oportunidades (2007 y 2011), tiene por objeto establecer una gestión integrada, mediante normas y procedimientos comunes, de control y vigilancia de las fronteras exteriores, corolario indispensable de la libre circulación de personas en la Unión Europea y componente esencial del espacio de Libertad, Seguridad y Justicia. Para ello, posee una base de datos que incluye, entre otros, datos personales de las personas que son devueltas a sus países de origen en las llamadas «operaciones de retorno», así como aquellas otras sospechosas de estar implicadas en actividades delictivas transfronterizas, en actividades de inmigración ilegal o en actividades de trata de personas. También regula el intercambio de datos personales con la Comisión, con los Estados Miembros, y con otras agencias de la Unión y organismos internacionales.

En lo que respecta al marco normativo aplicable al tratamiento de datos personales, hay que distinguir: si el tratamiento lo realiza Frontex en el cumplimiento de sus funciones , se aplican las disposiciones del Reglamento (CE) n° 45/2001. En cambio, si el tratamiento de datos lo realiza un Estado miembro en sus fronteras exteriores, esta materia pasa a estar directamente vinculada a la libre circulación de las personas en el espacio Europeo, y por tanto, le son plenamente aplicables también las disposiciones de la Directiva 95/46/CE, así como las normas generales y específicas que cada Estado haya dictado para regular la protección de datos en general, y en particular para la gestión y control de sus fronteras exteriores.

18. En los últimos años se han desarrollado un número importante de **sistemas informáticos de gran magnitud** (SIS, VIS, Eurodac, entre otros) vinculados directa o indirectamente a la supresión de las fronteras interiores de la Unión Europea. Aunque cada uno tiene un propósito diferente, estos sistemas de información comparten ciertas características comunes, tales como el tamaño y la interacción entre unidades nacionales, unidades centrales y con otros organismos de la Unión, e incluso con terceros países y organismos internacionales.

Con la finalidad de mejorar la gestión operativa de éstos sistemas de información, el Parlamento Europeo y el Consejo, mediante el Reglamento (UE) N° 1077/2011, de 25

de octubre de 2011, crearon una agencia europea para la gestión operativa a largo plazo de los sistemas informáticos de gran magnitud en el espacio de Libertad, Seguridad y Justicia (Eurosigma), que se encarga de la gestión operativa del Sistema de Información de Schengen de segunda generación (SIS II), del Sistema de Información de Visados (SIV) y de Eurodac.

El Tratamiento de los datos personales contenidos en dicha base de datos queda sometido al Reglamento 45/2001. No obstante, como cada uno de los sistemas de información que se incorpora a Eurosigma posee normas particulares sobre protección de datos, se estableció que la gestión operativa de este mega sistema informático no afecta a las normas específicas que regulan los principios, derechos, medidas de seguridad y otros requisitos de protección de datos aplicables a cada uno de los sistemas que lo compone. Por tanto, planteamos que la responsabilidad de garantizar y proteger los datos personales tratados en estos grandes sistemas de información debe recaer, en primer lugar, en el ente u órgano comunitario que proporciona o transfiere la información a esta nueva macro plataforma de gestión de datos; pero una vez transferida, debería ser la nueva agencia Eurosigma la que asuma la responsabilidad en el tratamiento de los datos personales bajo las condiciones y requisitos que le impone el Reglamento 45/2001. Con ello se logra una coherencia en la protección de los titulares de los datos, con el fin último de obtener un nivel de protección elevado y equivalente de los datos personales de las personas afectadas por dicho tratamiento, bajo cualquier sistema de gestión de datos para la prevención y represión penal.

Por otro lado, cabe señalar que el Sistema de Información Schengen surge primigeniamente como un mecanismo para la supresión de los controles fronterizos entre los Estados miembros. Posteriormente se le han ido agregando otras finalidades producto de varios factores: el aumento del número de países que integran la Unión Europea, los acelerados avances tecnológicos y las transformaciones institucionales y jurídicas que ha traído el Tratado de Lisboa.

Toda la normativa SIS, desde los primeros Acuerdos y Convenios, pasando por los Reglamentos y Directivas, contemplan un conjunto más o menos sistematizado y homogenizado de normas especiales sobre tratamiento de datos personales. No obstante, para determinar el **nivel mínimo de protección** a otorgar se recurría a los principios del Consejo de Europa en la materia, esto es, Convenio n° 108 del Consejo de Europa de 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, su protocolo adicional de 2001, y a la

Recomendación R (87) 15 de 17 de septiembre de 1987 del Comité de Ministros del Consejo de Europa, dirigida a regular la utilización de datos de carácter personal en el sector de la policía y sus modificaciones posteriores.

En lo que se refiere a la autoridad de control a cargo de supervisar el cumplimiento de la normativa del Sistema de Información Schengen, podemos indicar que existe una **concurrencia de autoridades competentes** que determinan su ámbito de acción en base, esencialmente, al *lugar de origen* y de *tratamiento* del dato personal. Así, se establece que las autoridades nacionales de control supervisen la legalidad del tratamiento de datos por los Estados Miembros, mientras que el Supervisor Europeo de Protección de Datos supervisa las actividades de las instituciones y los organismos comunitarios en relación con el tratamiento de datos personales.

Otro sistema de información de gran magnitud, con impacto directo en el tratamiento de datos personales con fines de prevención y represión penal, es el Sistema de Información de Visados (SIV). A diferencia del SIS, el SIV se estableció en el marco del antiguo primer pilar. No obstante, se adoptó un instrumento SIV en el tercer pilar para que los servicios policiales designados pudieran acceder al sistema, a fin de efectuar consultas relacionadas con la comisión de determinadas infracciones. Actualmente, la Autoridad de Gestión a cargo del SIV es la Agencia Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de Libertad, Seguridad y Justicia. En consecuencia, respecto del tratamiento de los datos personales realizados por el SIV, se aplica lo señalado respecto del SIS.

El último de los grandes sistemas de información analizados es el Sistema de Comparación de Huellas Dactilares (Eurodac). Originalmente, tenía por objeto determinar la identidad exacta de personas que solicitaban asilo o intentaban cruzar ilegalmente las fronteras exteriores de los Estados suscriptores. Posteriormente se le han ido agregando otras finalidades, vinculadas principalmente a la prevención y represión penal, entre las que destacan la lucha contra los delitos de terrorismo y otros delitos graves bajo el principio de disponibilidad. Actualmente su gestión operativa está a cargo de Eurosigma.

El **marco normativo aplicable a Eurodac**, se rige en primer lugar por las normas particulares sobre tratamiento de datos personales que contempla su regulación. Además, y dado que en su origen Eurodac fue creado en el antiguo primer pilar comunitario, le son plenamente aplicables las disposiciones de la Directiva 95/46/CE. Ahora bien, como se han agregado a sus fines materias propias del antiguo tercer pilar

comunitario, dichos tratamientos quedan sometidos a la protección que les brinda cada Estado miembro. Asimismo, por ser un organismo público europeo, le es plenamente aplicable las disposiciones del Reglamento n° 45/2000.

En cuanto a las autoridades encargadas de *controlar* y fiscalizar el respeto a las normas sobre protección de datos en Eurodac, nuevamente hay que realizar una distinción. Las autoridades nacionales de control supervisan la legalidad del tratamiento de datos personales realizados por las autoridades competentes de los Estados Miembros, destinadas a gestionar la utilización de huellas dactilares. Por su parte, el Supervisor Europeo de Protección de Datos es la autoridad competente, según lo dispuesto en el Reglamento (CE) n° 45/2001, para supervisar las actividades de Eurodac en relación con el tratamiento de datos personales.

19. Respecto del ámbito subjetivo del tratamiento de datos personales con fines de prevención y represión penal, es importante, en primer lugar, delimitar el concepto de **interesado**, esto es, toda persona física identificada o identificable, directa o indirectamente, por medios razonables por parte de cualquier persona física o jurídica, del objeto protegido, esto es, los datos personales. La claridad respecto de quiénes pueden ser las personas concernidas por un tratamiento con fines penales preventivos o represivos, así como los derechos que le asisten y las limitaciones o injerencias válidas de que pueden ser objeto éstos, es esencial para la adecuada defensa del derecho fundamental a la protección de datos.

Los interesados cuyos datos son tratados con fines de prevención y represión penal, pueden ser personas relacionadas directa o indirectamente con hechos delictivos, y en algunos casos, terceros no vinculados a ninguna con tales hechos. En cualquier caso, la participación en un ilícito no hace a las personas perder sus derechos fundamentales. En este sentido, la protección de datos personales opera como un **sistema de protección paralelo** al conjunto de derechos y principios del proceso penal.

Respecto del tratamiento de datos personales de las víctimas o presuntas víctimas de los delitos, destacamos la ausencia y, por tanto, la necesidad de incluir alguna disposición general sobre protección de la intimidad y datos personales que obligue a los Estados Miembros a garantizar a las víctimas sus derechos desde el primer contacto con las autoridades competentes. Lo anterior es plenamente aplicable, también, a otras terceras personas no involucradas directamente en los hechos delictivos, tales como los testigos, informantes o personas de contacto. La situación más delicada se vincula al

tratamiento de los datos de personas que no tienen ninguna relación, directa o indirecta, con un eventual ilícito penal. El tratamiento de datos de este tipo de interesado (personas no sospechosas) sólo se debería permitir cuando sea absolutamente necesario para un propósito legítimo, bien definido y específico. En todo caso, dicho tratamiento siempre deberá ser limitado en el tiempo y sólo para los fines que justificaron su recolección, prohibiéndose totalmente su uso posterior para fines distintos a los que motivaron su recolección.

Respecto del tratamiento de datos personales de menores de edad con fines de prevención y represión penal, y luego de revisar la normativa europea sobre protección de datos, concluimos que en la actual legislación vigente no se protege adecuadamente el interés superior del menor, situación que podría cambiar con la entrada en vigencia de la propuesta de nuevo Reglamento General sobre protección de datos, donde se les destina un artículo específico a proteger a los menores, de acuerdo a los estándares y compromisos internacionales en la materia. No obstante, en el ámbito específico de la prevención y represión penal, la protección de los niños, niñas y adolescentes queda bastante mermada, ya que no se les brinda ninguna protección especial en relación a la protección de sus datos personales.

20. En cuento a los **derechos de los interesados** en el tratamiento de los datos personales con fines de prevención y represión penal, ha existido una evolución y perfeccionamiento de estos, ya que se pasó de una regulación de mínimos a la determinación de una mayor cantidad de facultades inherentes al derecho a la protección de datos personales, entre las que se encuentran los derechos a la información, acceso, rectificación, cancelación, oposición, a presentar un recurso y a ser indemnizado. Cada uno de estos derechos o facultades inherentes a la protección de datos ha recibido un tratamiento particular por parte del legislador europeo en lo relativo a su reconocimiento, condiciones de ejercicio, así como a sus límites y excepciones.

21. La primera facultad que otorga el derecho a la protección de datos al titular de los datos personales es el **derecho a ser informado** sobre la recolección, registro y uso que se les dará a éstos. Este derecho tiene como contrapartida la obligación de los responsables del tratamiento de informar al interesado, entre otros extremos, sobre los puntos indicados. En el ámbito específico de la prevención y represión penal, la legislación vigente (Decisión Marco 2008/977/JAI) en su artículo 16 impone a los Estados Miembros la

obligación de informar al titular de los datos respecto de los tratamientos que se estén llevando a cabo. No obstante, el ejercicio del derecho queda supeditado a lo dispuesto en la legislación de cada uno de los Estados Miembros, lo que puede generar disparidad de criterios en cuanto al nivel de protección que se brinda al mismo.

Esta situación podría cambiar si se aprueba la propuesta de Directiva que pretende derogar y reemplazar la Decisión Marco citada, ya que aquella contempla un articulado mucho más explícito y detallado sobre el derecho a la información (artículo 11 de la propuesta de Directiva COM (2012) 10 final de 25.1.2012), el que, junto con establecer la obligación de los Estados Miembros de garantizar la información al interesado, amplía y detalla cuál es la información que se le debe entregar al titular de los datos.

Uno de los principales problemas en relación al derecho a la información en el ámbito de la investigación policial, es determinar cuál es el *momento* adecuado en que debe informarse al titular de los datos que está siendo objeto de una medida de tratamiento de sus datos personales. Se trata de conciliar, por un lado, el éxito de la investigación (seguridad), y por otro, los derechos del titular de los datos (libertad). Como criterio general de solución a este conflicto, se ha establecido por la jurisprudencia del TEDH, que se pueden tratar datos personales sin conocimiento del interesado en la medida que exista un control judicial previo (autorización), que dichas medidas (tratamiento) sean compatibles con las garantías del CEDH, y que se le informe al interesado sobre dichas medidas una vez que éstas hubieren concluido.

22. Otra facultad esencial que integra el derecho a la protección de datos es el **derecho de acceso**, que permite al titular de los datos consular cualquier información sobre su persona que haya sido introducida en un fichero o base de datos, así como el origen de la misma, la finalidad del tratamiento y los destinatarios o categorías de destinatarios a quienes se hayan transmitido o pretendan comunicar dichos datos. Esta facultad de la protección de datos no debe confundirse con el derecho de acceso a la información contenida en archivos, registro o documentos de instituciones u organismos públicos, ya que ambos tienen fines u objetos diversos.

Respecto del tema específico de nuestra tesis, el derecho de acceso está regulado tanto en la Recomendación (87) 15 del Consejo de Europa, como en la Decisión Marco 2008/977/JAI de la Unión Europea. Ésta última establece el tipo de información que puede solicitar el interesado, la que se reduce a confirmar si se han transmitido o puesto a disposición datos que le conciernen; información sobre los destinatarios o categorías

de destinatarios a los que se han remitido los datos; y la comunicación de los datos que se están tratando. Además, se regulan los supuestos bajo los cuales se puede *limitar* o *denegar* el derecho de acceso. En tales casos, junto con tomar en cuenta los intereses legítimos del interesado, la medida debe ser necesaria y proporcionada en relación a los fines de prevención o sanción penal perseguidos.

La propuesta de Directiva, que pretende derogar y reemplazar a la Decisión Marco, consagra también el derecho de acceso, pero adiciona otros aspectos que se deben informar al interesado, tales como el periodo de conservación y los derechos que le asisten. En cuanto a la limitación de este derecho, la propuesta sigue con lo dispuesto en la Decisión Marco, sin innovar demasiado sobre el punto.

Como apreciación general, podemos indicar que el derecho de acceso se encuentra en una mejor posición en la actualidad en el sistema europeo, no obstante, la regulación de sus límites y excepciones sigue siendo demasiado laxa, lo que afecta el necesario equilibrio entre seguridad y libertad que está en juego en el tratamiento de datos personales en el ámbito de prevención y represión penal.

23. Otro derecho que integra las facultades inherentes a la protección de datos, es la **rectificación**, el cual permite la corrección de los datos incompletos o inexactos. Este se encuentra directamente relacionado con el principio de veracidad o calidad de los datos, ya que ambos buscan que el tratamiento de éstos refleje la realidad. Criticamos la regulación que realiza de este derecho la Decisión Marco, porque la redacción del artículo 4 da la impresión que deja al arbitrio de los Estados Miembros el rectificar los datos incorrectos, lo que no se condice con la importancia que tiene para el tratamiento de los datos con fines penales que estos sean efectivamente actualizados. Por otra parte, también es criticable que la Decisión Marco deje al criterio de cada Estado la regulación sobre el ejercicio de este derecho, ya que evidentemente se generan diferentes estándares para los titulares de los datos de los diversos países miembros de la Unión.

Por otro lado, la propuesta de Directiva que reemplazaría la actual legislación vigente sobre protección de datos en el ámbito de la cooperación policial y judicial, reconoce la rectificación tanto como un derecho para el titular de los datos, como una obligación para los Estados Miembros. No obstante, tanto la Decisión Marco como la propuesta de Directiva remiten al derecho nacional de cada Estado para la regulación de este derecho, lo que, como hemos venido sosteniendo, puede generar disparidad de criterios que afecten a los titulares de los datos de los diferentes Estados Miembros.

Respecto del derecho de **oposición**, señalamos que en el ámbito específico de la cooperación policial y judicial, no existe ninguna referencia a este derecho, a diferencia de lo que ocurre con la legislación en el ámbito del antiguo primer pilar comunitario, donde sí se encuentra regulada.

24. En cuanto al **derecho de supresión, cancelación o borrado**, señalamos que procedía cuando el tratamiento carecía de una base de legitimación. En el ámbito específico de la prevención y represión penal, dichos datos deberían ser suprimidos cuando ya no sean necesarios para los fines que fueron legalmente recogidos y tratados. No obstante, la Decisión Marco 2008/977/JAI permite a los Estados quebrar este principio general, bajo la condición de que los datos estén contenidos de manera independiente por un periodo de tiempo adecuado, de acuerdo a su legislación nacional. Criticamos esta disposición porque introduce un concepto ambiguo como lo es *«un periodo de tiempo adecuado»*, cuya extensión queda, en definitiva, a criterio de cada Estado miembro. Como forma de superar dicho problema proponemos que el tratamiento en ningún caso pueda exceder del tiempo necesario para que opere la **prescripción** de los delitos.

La propuesta de Directiva que pretende reemplazar a la Decisión Marco se inspira en la Directiva 95/46/CE, pero no innova mayormente en la materia, salvo tres supuestos donde se permite «marcar» los datos en vez de suprimirlos. Estos son: a) que el interesado impugne su exactitud, durante un plazo que permita al responsable del tratamiento verificar la exactitud de dichos datos; b) que los datos personales hayan de conservarse a efectos probatorios; c) que el interesado se oponga a su supresión y solicite la limitación de su uso.

25. Otra de las facultades incluidas en el derecho a la protección de datos es el derecho a solicitar, por parte del interesado, el **bloqueo** de éstos. En el ámbito del tratamiento de datos personales con fines de prevención o represión penal, se ha definido el bloqueo como la señalización o marcado de datos personales conservados con el objetivo de limitar su tratamiento en el futuro. Los datos personales se bloquean en lugar de suprimirse cuando haya razones fundadas para suponer que la supresión podría afectar los intereses legítimos del interesado, permitiéndose en tales casos el tratamiento sólo para los fines señalados en el bloqueo.

La propuesta de Directiva COM (2012) 10 final de 2012, elimina el concepto de bloqueo por considerarlo ambiguo, y en su lugar, utiliza la expresión "**marcado**" o

"**restricción**" del tratamiento. Sea cual sea la terminología utilizada, para nosotros el propósito es el mismo: limitar el uso de los datos única y exclusivamente para los fines que impidieron su supresión o cancelación.

26. En cuanto al **derecho al recurso**, cabe destacar dos ideas. La primera, dice relación con el desarrollo que ha tenido este derecho tanto en la propuesta de Reglamento General de Protección de datos, como en la propuesta de Directiva para el ámbito de la prevención y represión penal. En efecto, se pasa de una regulación mínima o básica si se quiere, a una regulación más detallada, distinguiendo si el recurso es de carácter administrativo o jurisdiccional. Además, se extiende el derecho a presentar una reclamación ante una autoridad de control en *cualquier* Estado miembro y a presentar un recurso judicial si considera que se vulneran sus derechos en el marco de la presente Directiva, o en caso de que la autoridad de control no reaccione ante una reclamación o no actúe cuando dicha medida sea necesaria para proteger los derechos del interesado.

También es importante destacar que el derecho a presentar un recurso se extiende tanto a las personas físicas como *jurídicas* y, particularmente, dentro de éstas últimas, a toda entidad, organización o asociación que tenga por objeto proteger los derechos e intereses de los interesados en relación con la protección de sus datos.

27. Por último, el interesado tiene derecho a que se **indemnice** por los perjuicios de cualquier naturaleza que se hubiesen provocado como consecuencia de un tratamiento ilegal de los datos personales. Así lo recoge tanto la Decisión Marco 2008/977/JAI (artículo 19.1), como la propuesta de Directiva de 2012 (artículo 54.1). La propuesta de Directiva innova sólo respecto del sujeto responsable de los daños, ya que amplía lo dispuesto en la Decisión Marco, haciendo extensiva dicha responsabilidad en forma *solidaria* tanto a los responsables, como a los encargados, sean estos uno o varios sujetos.

28. Respecto de los **límites y excepciones** al derecho a la protección de datos en el ámbito específico de la prevención y represión penal, señalamos que este derecho, como cualquier otro, puede ser objeto de injerencias, ya sea producto de su interrelación con otros derechos, ya sea por la necesidad de satisfacer otros bienes y valores jurídicos relevantes en una sociedad democrática. No obstante, para que dichas limitaciones y excepciones sean toleradas, se deben cumplir ciertos estándares propios de un Estado

democrático de derecho, con la finalidad de precaver posibles afectaciones arbitrarias a los derechos fundamentales.

Siguiendo la jurisprudencia del TEDH y del TJUE, llegamos a la conclusión que pueden establecerse restricciones al ejercicio de estos derechos, siempre que dichas restricciones respondan efectivamente a objetivos de interés general perseguidos por la comunidad y no constituyan, teniendo en cuenta el objetivo perseguido, una intervención desmesurada e intolerable que afecte a la esencia misma de dichos derechos.

Ahora bien, en el ámbito específico de nuestro estudio, pudimos constatar que la actual Decisión Marco vigente remite al *derecho nacional* la regulación de los límites y excepciones al ejercicio de los derechos que emanan de la protección de datos personales, y sólo hace referencia expresa a la materia a propósito de la transferencia de datos entre Estados Miembros de la Unión, que estén sometidos a una limitación particular por parte del Estado transmitente. Señalamos que la regulación es, a todas luces, insuficiente, por cuanto las transferencias internacionales de datos personales con fines de represión y sanción penal son cada día más habituales y necesarias en la sociedad europea actual.

Por su parte, la propuesta de Directiva que pretende sustituir la Decisión Marco, remite también la materia de los límites y excepciones al ejercicio de los derecho a la legislación de cada Estado miembro de la Unión, dedicando sólo una disposición particular para la regulación los límites al derecho de acceso, cuyos criterios quedan establecidos en el artículo 13 de la propuesta.

Pensamos que no existen razones para no haber extendido dicha regla al resto de las facultades que emanan de la protección datos, y que en un próximo periodo de revisión de dicho instrumento se debería evaluar su incorporación como una norma de carácter general. Por último, no debemos olvidar que toda injerencia a un derecho fundamental debe tener en cuenta lo que se ha denominado como *«test democrático de restricción de derechos»*, es decir, que este previsto en una ley, que exista una necesidad o interés general que lo justifique, que no afecte el contenido esencial de los derechos afectados, y que la injerencia en el derecho sea proporcionada en relación a los fines que se pretenden alcanzar.

29. La preocupación por las **transferencias internacionales de datos personales** ha sido una constante en las diversas legislaciones sobre protección de datos aprobadas por el

legislador europeo. Dado que el poder de control sobre los datos personales por parte de su titular disminuye sensiblemente si éstos son transferidos a terceros Estados u organismos internacionales situados fuera de la Unión, se han tratado de idear mecanismos por los cuales se pueda garantizar que dichos datos seguirán teniendo un nivel de protección adecuado, una vez que sean transferidos fuera de la frontera física o virtual de los Estados Miembros. La Directiva 95/46/CE, regula la transferencia internacional de datos personales a terceros Estados y a organismos internacionales, pero su ámbito de aplicación no abarca los datos personales tratados en el ámbito de la cooperación penal y judicial, por corresponder al antiguo tercer pilar comunitario.

Dicha falencia se suplió parcialmente con la aprobación de la Decisión Marco 2008/977/JAI, ya que ésta contiene en un solo artículo los requisitos y condiciones necesarias para proceder a autorizar una transferencia internacional de datos personales con fines de prevención o sanción penal. La forma cómo están reguladas las transferencias internacionales de datos en la Decisión Marco es **insuficiente**, ya que sólo contempla el supuesto de una transferencia realizada de un Estado de la Unión que ha recibido previamente los datos de otro Estado miembro, dejando así a criterio de cada Estado la forma de regular las transferencias internaciones de datos con fines de cooperación policial y judicial en materias penales.

La propuesta de Directiva COM (2012) 10 final, que pretende sustituir y derogar la Decisión Marco 2008/977/JAI, introduce una serie de modificaciones respecto de los términos en que se puede llevar a cabo una transferencia internacional de datos personales con fines de prevención y sanción penal. De partida, llaman la atención las múltiples opciones de transferencia que van desde la más estricta, esto es, el cumplimiento de una nivel adecuado de protección por parte del país u organismo internacional, hasta llegar a una serie de *excepciones* donde se permiten las transferencia sin ningún tipo de garantía. En una zona intermedia, queda la posibilidad de transferir datos a destinos que no cumplan con un nivel adecuado de protección si se otorgan las garantías adecuadas o se ha suscrito un acuerdo internacional que contemple algún tipo de transferencia.

Una novedad que plantea la propuesta en relación al nivel de protección, es la facultad que se le otorga a la Comisión de declarar con nivel de protección adecuado no sólo a un tercer país u organismo internacional, sino también a *sectores específicos* o *territorios determinados* de un tercer país. Además, la decisión de adecuación puede ser genérica o específica.

La propuesta de Directiva establece una serie de requisitos y condiciones para declarar que el lugar de destino de los datos posee un **nivel adecuado de protección**. En primer lugar, y tomando como parámetro los principios fundamentales de la Unión, exige que en el lugar de destino se garantice el Estado de Derecho y el acceso a la justicia. Otro requisito para declarar adecuado el nivel de protección, es la existencia y funcionamiento efectivo, en el lugar de destino, de una o varias autoridades de control. Un tercer elemento a considerar por la Comisión para declarar el nivel adecuado de protección, son los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate. Cumplidos todos los requisitos, la Comisión declarará que el país u organismo internacional cuenta con un nivel de protección adecuado. En caso contrario, se prohíbe a todos los países miembros de la Unión transferir datos a dichos destinos que no cuenten con él.

Ahora bien, aun cuando el lugar de destino no ofrezca garantías en cuento a nivel adecuado, la Directiva permite dicha transferencia si se garantiza apropiadamente la transferencia por parte del tercer país u organismo internacional. La formas de acreditar o demostrar dichas **garantías suficientes** puede darse por dos vías: la primera, a través de un acuerdo internacional jurídicamente vinculante, y la segunda, es que el responsable o el encargado del tratamiento evalúe todas las circunstancias que concurren en la transferencia de datos personales, y lleguen a la conclusión de que existen garantías apropiadas con respecto a la protección de datos personales. Criticamos esta última alternativa, porque la evaluación no la hace la autoridad de control de protección de datos, sino la autoridad competente en materia judicial o policial, por tanto, es probable que exista una propensión a facilitar la cooperación policial y judicial por sobre el respeto efectivo de las garantías fundamentales, entre las que se encuentra la protección de datos. La autoridad a cargo en materia de control de datos en estos casos sólo actúa *ex post*, es decir, una vez que se ha producido la transferencia internacional.

La propuesta de Directiva, al igual que la Decisión Marco 2008/977/JAI y la Directiva 95/46/CE, contempla una serie de casos o hipótesis en que se permite las transferencias de datos personales sin ningún tipo de requisito o exigencia. Dichas situaciones miran generalmente a los intereses de los titulares de los datos, como también a intereses sociales preponderantes donde el derecho a la protección de datos cede ante un bien jurídico colectivo de mayor entidad.

Por último, y con la finalidad de hacer frente a una serie de problemas que trae aparejado la transferencia internacional de datos, tanto para el titular de los datos como para las autoridades de control, se han establecido en la propuesta de Directiva una serie de mecanismos que buscan reforzar la *cooperación* entre las autoridades encargadas de la protección de datos personales.

30. Un caso crítico que desnuda todos los problemas del sistema internacional de tratamiento de datos es el del **Registro de Nombre de Pasajeros** (*Passenger Name Record* - PNR). El contexto en que surgen y se desarrollan éstas y otras medidas de seguridad nacional son los atentados terroristas ocurridos en Estados Unidos de Norteamérica (2001), España (2004) y Reino Unido (2005). A partir de ello ha existido un progresivo y continuo aumento de las medidas legales destinadas a combatir la amenaza terrorista, entre las cuales se encuentra el uso de los datos personales que gestionan las aerolíneas en el proceso de reserva y venta de pasajes.

Un hito importante en el proceso de celebración de este tipo de Acuerdos celebrados entre la Unión Europea y terceros Estados, lo constituye el **fallo del TJUE** que anula de las Decisiones que aprobó la celebración del acuerdo entre la UE y EE.UU. sobre transferencia de datos del PNR. En dicho fallo se encuentra claramente establecido que la transferencia de los datos de los PNR constituye un tratamiento que tiene por objeto la *seguridad pública* y las actividades del Estado en materia penal. Por tanto, aunque los datos sean recolectados por privados para la realización de una prestación de servicios (compañías aéreas, en este caso) en el marco de una actividad regulada por el Derecho comunitario, lo que determinará la normativa aplicable (estatal y europea de protección de datos) es la *naturaleza* del tratamiento.

Es importante que tanto la futura normativa europea que regule el PNR, como la suscripción ó renovación de nuevos Acuerdos con terceros países, fije claramente los **fines** para los cuales serán utilizados los registros de nombres de pasajeros. Sobre este punto planteamos dos opciones: *limitar* la transmisión de los datos del PNR sólo para delitos terroristas y formas graves de delincuencia organizada de carácter transnacional. La otra sería la suscripción de un *Acuerdo internacional* sobre cooperación policial y judicial que incluyese otros supuestos, pero tomando las cautelas necesarias en relación a establecer un adecuado nivel de protección de los derechos y libertades fundamentales. Es necesario avanzar hacia un acuerdo global de transferencia de datos personales para fines preventivos y represivos en el ámbito de la cooperación policial y

judicial en materia penal. En esta línea se encuentra la Propuesta de Resolución del Parlamento Europeo sobre enfoque global del PNR y la subscripción de un nuevo acuerdo entre la UE y EE.UU., Australia y Canadá

31. Lo anterior nos lleva a una reflexión final sobre los **términos** de la lucha contra el terrorismo internacional. Es necesario que ésta sea limitada y definida, ya que de lo contrario, al establecerse unos fines amplios o laxos, se permitirían injerencias injustificadas al derecho a la privacidad y a otros derechos y libertades fundamentales. En ésta línea, la cooperación policial, por medio del intercambio y disponibilidad de datos de carácter personal de los ciudadanos, debe darse respetando un nivel mínimo de garantías en favor de la persona concernida (afectada). Sólo el respeto de estos principios, derechos y obligaciones establecidos para el tratamiento de los datos personales, impedirá que la lucha contra la delincuencia (grave o no) socave los fundamentos del Estado democrático de Derecho y el respeto de los derechos fundamentales que con tanto esfuerzo se ha construido en Europa a partir de la segunda mitad del siglo XX.

Fin.

A)

A efectos policiales: abarca todas las tareas que las autoridades de policía debe realizar para la prevención y represión de los delitos y el mantenimiento del orden público

Acervo comunitario: los derechos y obligaciones que comparten los países de la Unión Europea, lo que incluye todos los tratados, normas, declaraciones y resoluciones de la UE., sus acuerdos internacionales y las sentencias dictadas por el Tribunal de Justicia.

Actos públicos: Son actos públicos aquellos que tienen lugar ante un número indeterminado de personas, lo organice quien lo organice, se consideran actos públicos, caracterizados por presentar un notable alcance ante la sociedad, bien porque se produzcan ante un gran número de personas o bien porque los medios de comunicación presentes lo difundan ante una gran masa social

Acuerdo y convenio de Schengen: El Acuerdo de Schengen, firmado el 14 de junio de 1985 entre Alemania, Bélgica, Francia, Luxemburgo y los Países Bajos, tiene por objeto eliminar progresivamente los controles en las fronteras comunes y establecer un régimen de libre circulación para todos los nacionales de los Estados signatarios, de los otros Estados de la Comunidad o de terceros países. El Convenio de Schengen completa el Acuerdo y define las condiciones y las garantías de aplicación de esta libre circulación. Este Convenio, firmado el 19 de junio de 1990 por los mismos Estados miembros, no entró en vigor hasta 1995. El Acuerdo y el Convenio, así como las normas y acuerdos conexos conforman el «acervo de Schengen». Desde 1999, el acervo de Schengen está integrado en el marco institucional y jurídico de la Unión Europea en virtud de un protocolo anexo a los Tratados.

ADN: el ácido desoxirribonucleico, frecuentemente abreviado como ADN (y también DNA, del inglés *Deoxyribonucleic Acid*), es un ácido nucleico, una macromolécula que forma parte de todas las células. Contiene la información genética usada en el desarrollo y funcionamiento de los organismos vivos conocidos y de algunos virus, siendo el responsable de su transmisión hereditaria.

Archivo: el término archivo (del latín *archivum*) se usa comúnmente para designar el local donde se conservan los documentos producidos por otra entidad como consecuencia de la realización de sus actividades. Los archivos son el conjunto organizado de informaciones del mismo tipo, que pueden utilizarse en un mismo tratamiento; como soporte material de estas informaciones. // **Archivo o fichero informático:** conjunto de información organizado y grabado como una unidad en un soporte informático de almacenamiento.

Autenticación: proceso por el cual se revelan aspectos de la identidad de una persona.

Autodeterminación informativa: se ha definido como el derecho del individuo a controlar la obtención, tenencia, tratamiento y trasmisión de datos relativos a su persona, decidiendo en cuanto a los mismos, las condiciones en que dichas operaciones pueden llevarse a cabo.

Autoridad de control: la autoridad pública establecida por un Estado miembro de acuerdo con el artículo 39 (propuesta Directiva COM 2012/0010 Final). / (2) La autoridad pública establecida por un Estado miembro de acuerdo con el artículo 46. (Propuesta Reglamento de Directiva COM 2012/0011 Final)

Autoridades competentes: toda autoridad pública competente para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales (propuesta Directiva COM 2012/0010 Final). / (2) Los servicios u organismos creados en virtud de actos jurídicos adoptados por el Consejo al amparo del título VI del Tratado de la Unión Europea, así como las autoridades policiales, judiciales, aduaneras y otras autoridades competentes de los Estados miembros autorizadas por el Derecho nacional a tratar datos personales en el ámbito de la presente Decisión Marco. (Decisión Marco 2008/977/JAI)

B)

Bloqueo: el marcado de los datos almacenados de carácter personal con el fin de limitar su tratamiento en el futuro.

C)

Consulta automatizada: el acceso directo a una base de datos automatizada de otra instancia, de tal forma que pueda obtenerse respuesta a la consulta de forma totalmente automática.

Consentimiento del interesado: toda manifestación de voluntad, libre, específica, informada y explícita, mediante la que el interesado acepta, ya sea mediante una declaración ya sea mediante una clara acción afirmativa, el tratamiento de datos personales que le conciernen (Propuesta Reglamento COM 2012/0011 final)

Cooperaciones reforzadas: permite una colaboración más estrecha entre los países de la Unión que deseen seguir profundizando en la construcción europea, respetando el marco jurídico de la Unión. De este modo, los Estados miembros interesados pueden progresar según ritmos u objetivos diferentes. No obstante, la cooperación reforzada no permite ampliar las competencias previstas por los Tratados ni puede aplicarse a ámbitos que sean competencia exclusiva de la Unión. Además, solo puede iniciarse como último recurso, en caso de que haya quedado sentado en el seno del Consejo que los objetivos asignados no pueden ser alcanzados por el conjunto de la Unión en un plazo razonable.

D)

Datos personales: toda información sobre una persona física identificada o identificable («el interesado»). Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social (Decisión Marco 2008/977/JAI). / (2) Toda información relativa a un interesado (Propuesta Reglamento COM 2012/0011 final)

Datos genéticos: todos los datos, con independencia de su tipo, relativos a las características de una persona que sean hereditarias o adquiridas durante el desarrollo prenatal temprano;

Datos biométricos: cualesquiera datos relativos a las características físicas, fisiológicas o conductuales de una persona que permitan su identificación única, como imágenes faciales o datos dactiloscópicos;

Datos relativos a la salud: cualquier información que se refiera a la salud física o mental de una persona, o a la asistencia prestada por los servicios de salud a la persona;

Decisión: la decisión se utiliza para cualquier objetivo distinto de la aproximación de las disposiciones legislativas y reglamentarias de los Estado miembros. Es vinculante y las medidas necesarias para aplicarla a escala de la Unión Europea se adoptan por el consejo por mayoría cualificada. Con la supresión del tercer pilar prevista en la Constitución Europea, actualmente en proceso de ratificación, las decisiones y decisiones marco que ahora se utilizan van a desaparecer y serán sustituidas por leyes y leyes marco europeas.

Decisión marco: se utiliza para aproximar las disposiciones legislativas y reglamentarias de los Estados miembros de la UE. Propuesta a iniciativa de la Comisión o de un Estado miembro, debe ser adoptada por unanimidad. Vincula a los Estados miembros en cuanto a los resultados que deben alcanzarse y deja a las instancias nacionales la decisión sobre la forma y los instrumentos necesarios para alcanzarlos

Derecho a la privacidad: el derecho a la privacidad es el derecho del individuo para decidir por sí mismo en qué medida compartirá con los demás sus pensamientos, sus sentimientos y los hechos de su vida personal como asimismo el derecho a decidir sobre el desarrollo de su personalidad, mientras no dañe a terceros, siempre que sus actuaciones no sean de relevancia pública, ni contravengan el ordenamiento público.

Destinatario: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos personales (Propuesta Reglamento COM 2012/0011 final)

E)

Espacio y cooperación de Schengen: se basan en el Tratado de Schengen de 1985. El espacio Schengen representa un territorio donde está garantizada la libre circulación de las personas. Los Estados que firmaron el tratado han suprimido todas las fronteras interiores y en su lugar han establecido una única frontera exterior, aplicando

procedimientos y normas comunes en lo referente a los visados para estancias cortas, las solicitudes de asilo y los controles fronterizos. Al mismo tiempo, ha intensificado la cooperación y la coordinación entre los servicios policiales y las autoridades judiciales para garantizar la seguridad dentro del espacio Schengen.

Empresa: toda entidad dedicada a una actividad económica, independientemente de su forma jurídica, incluidas, en particular, las personas físicas y jurídicas, así como las sociedades o asociaciones que ejerzan regularmente una actividad económica;

Encargado del tratamiento: la persona física o jurídica, autoridad pública o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento. / (2) Todo organismo que trate datos personales por cuenta del responsable del tratamiento.

Establecimiento principal: en lo que se refiere al responsable del tratamiento, el lugar de su establecimiento en la Unión en que se adopten las decisiones principales en cuanto a los fines, condiciones y medios del tratamiento de datos personales; si no se adopta en la Unión decisión alguna en cuanto a los fines, condiciones y medios del tratamiento de datos personales, el establecimiento principal es el lugar donde tienen lugar las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del responsable del tratamiento en la Unión. Por lo que respecta al encargado del tratamiento, por establecimiento principal se entiende el lugar de su administración central en la Unión.

Eurojust: es una agencia de la Unión Europea encargada de intensificar la lucha contra las formas graves de delincuencia gracias a una cooperación judicial más estrecha en el seno de la Unión Europea. Formada por 27 representantes nacionales: jueces fiscales y policías asignados por cada país miembro. Puede llevar a cabo su labor bien por mediación de uno o varios de los miembros nacionales afectados, bien de forma colegiada.

Europol: es una agencia de la Unión Europea encargada de mejorar la cooperación entre las autoridades policiales y los servicios de seguridad de los Estados miembros.

F)

Fichero: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica

Fichero automatizado: cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado (convenio 108). / (2) Se refiere a todo conjunto organizado de datos de carácter personal que permita acceder a la información relativa a una persona física determinada utilizando procesos de búsqueda automatizados. (Extraído de cuidatusdatos.com)

Flujos transfronterizos de datos personales: se entienden los desplazamientos de datos personales más allá de las fronteras nacionales.

Frontex: Agencia europea para la gestión de la cooperación operativa en las fronteras exteriores de los Estados miembros de la Unión.

G)

Grupo de trabajo del artículo 29: creado en virtud del artículo 29 de la Directiva 95/46/CE. Es un órgano consultivo independiente de la Unión Europea, que se pronuncia sobre los temas vinculados a la protección de datos y la vida privada. Sus tareas se definen en el artículo 30 de la Directiva 65/46/CE y en el artículo 14 de la directiva 97/66/CE.

H)

Habeas Data: es una acción que asiste a una persona identificada o identificable para solicitar judicialmente la exhibición de los registros -públicos o privados- en los cuales está incluidos sus datos personales o los de su grupo familiar, para tomar conocimiento acerca de su exactitud.

Huella abierta: Los índices de referencia con perfiles de ADN que no puedan atribuirse a ninguna persona

Huella genética: es una técnica utilizada para distinguir entre los individuos de una misma especie utilizando muestras de su ADN

I)

Interesado: toda persona física identificada o que pueda ser identificada, directa o indirectamente, por medios que puedan ser utilizados razonablemente por el responsable del tratamiento o por cualquier otra persona física o jurídica, en particular mediante un número de identificación, datos de localización, identificador en línea o uno o varios elementos específicos de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

L)

Libertad informática: Vittorio Frosini la define como un derecho de autotutela de la propia identidad informática, es decir, el derecho de controlar (conocer, corregir, quitar o agregar) los datos personales inscritos en las tarjetas de un programa electrónico.

M)

Marcado: la señalización de datos personales conservados sin el objeto de limitar su tratamiento en el futuro. / (2) La inserción de una marca en los datos almacenados de carácter personal sin que con ello se pretenda limitar su tratamiento en el futuro.

N)

Niño: Toda persona menor de 18 años

O)

Órgano competente: denota la autoridad, servicio o cualquier otro organismo público que sea competente conforme a la ley nacional para decidir sobre la finalidad de un fichero automatizado, las categorías de datos personales que deben ser almacenados y las operaciones que se aplican a ellos.

P)

Pasaporte biométrico: también conocido como pasaporte electrónico, es un documento de identidad que además del uso de papel de seguridad, contiene una lámina de policarbonato con un circuito electrónico incrustado en ella, y que usa la biometría para autentificar la ciudadanía de los viajeros. La incorporación de un minúsculo chip RFID en el documento permite tanto almacenar información adicional como duplicarla que se encuentra impresa en la página que contiene los datos del titular del pasaporte, permitiendo –a través de infraestructura de clave pública- la certificación de la veracidad de los datos contenido en él, haciendo virtualmente imposible forjar identidades falsas.

Perfiles: un método informatizado que, mediante la prospección de un gran banco de datos, permita o tenga por objeto permitir clasificar a una persona en una categoría determinada, con cierta probabilidad (y por tanto, con cierto margen de error), a fin de tomar respecto de ella decisiones individualizadas.

PET (Tecnologías de protección de la intimidad): son un sistema coherente de medidas de TIC que protege el derecho a la intimidad suprimiendo o reduciendo los datos personales o evitando el tratamiento innecesario o indeseado de datos personales, sin menoscabo de la funcionalidad del sistema de información.

Pilares comunitarios: El Tratado de Maastricht (1992) introdujo una nueva estructura institucional a la Unión Europea que se mantuvo hasta la entrada en vigor del Tratado de Lisboa. Dicha estructura institucional estaba compuesta por tres «pilares»: el pilar comunitario (primer pilar), que correspondía a las tres comunidades: la Comunidad Europea, la Comunidad Europea de la Energía Atómica (Euratom) y la antigua Comunidad Europea del Carbón y del Acero (CECA) (primer pilar); el pilar correspondiente a la política exterior y de seguridad común (segundo pilar), que estaba regulada en el título V del Tratado de la Unión Europea (segundo pilar); el pilar correspondiente a la cooperación policial y judicial en materia penal (tercer pilar), cubierta por el título VI del Tratado de la Unión Europea. El Tratado de Ámsterdam transfirió una parte de las competencias del tercer pilar al primero (libre circulación de personas). Estos tres pilares funcionaban siguiendo procedimientos de decisión diferentes: procedimiento comunitario para el primer pilar y procedimiento intergubernamental para los otros dos. El Tratado de Lisboa elimina esta estructura de pilares en beneficio de la creación de la Unión Europea (UE). En la UE, las decisiones se adoptan con arreglo a un procedimiento de Derecho común denominado «procedimiento legislativo ordinario». Sin embargo, el método intergubernamental sigue aplicándose a la política exterior y de seguridad común. Por otra parte, aunque las cuestiones relativas a justicia e interior se encuentran «comunitarizadas», algunas de ellas, en especial relacionadas con la cooperación policial y judicial en materia penal, siguen sujetas a procedimientos especiales en los cuales los Estados miembros conservan poderes importantes. Tal como se habían configurado formalmente a partir

del Tratado de Amsterdam (1997), y gestados previamente a partir del Tratado de Maastricht, por lo que los actos de la Unión en el ámbito de la cooperación policial y judicial en asuntos penales pasa a formar parte del espacio de libertad, seguridad y justicia.

PNR: *Passenger Name Records* (PNR) o registro de nombres de pasajeros, es un registro de los requisitos de viaje que contiene toda la información necesaria para que sea posible la tramitación y el control de reservas por parte de todas las compañías aéreas que las realizan y participan en el registro// Información no verificada que proporcionan los pasajeros y recogen las compañías aéreas para efectuar las reservas y llevar a cabo el proceso de facturación. Se trata de un registro de los requisitos de viaje de cada pasajero que figura en los sistemas de reservas y control de salidas de las compañías. Contiene diversos tipos de información, por ejemplo las fechas y el itinerario de viaje, los datos del billete, datos de contacto, agencia de viajes, información sobre el pago, número de asiento y datos del equipaje.

Principio de acceso equivalente: se refiere al tratamiento de las peticiones de información sea de acuerdo a las condiciones del Estado miembro requerido

Principio de disponibilidad: este nuevo concepto implica que las autoridades policiales de un Estado miembro pueda acceder a la información de las autoridades de otro Estado miembro, con el fin de impedir un delito, de detectar infracciones penales o a efectos de investigación.

Principio de ponderación de los derechos: es aquel en donde la situación de igualdad inicial de los derechos en conflicto se rompe en beneficio de uno de ellos en virtud de condiciones o circunstancias específicas del mismo, haciendo que dicho derecho prevalezca

Principio de unidad de la Constitución: este principio exige que el legislador realice el máximo esfuerzo por configurar y regulara los derechos en un sistema donde cada uno de ellos colisione lo menos posible con otros, donde los derechos constituyan círculos tangentes y no círculos secantes que se invadan unos a otros, lo que exige la adecuada ponderación y un eventual sacrificio mínimo de cada derecho que exige el principio de proporcionalidad que debe emplear necesariamente el legislador en la regulación de los derechos.

Privacidad: ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión. / (2) La privacidad constituye como los demás derechos una derivación de la dignidad de la persona humana, consistente en la creación y control de espacios vedados al público, constituyendo un perímetro de garantía frente a intromisiones de terceros no deseados por la persona, protegiéndolo de intromisiones informativas (conocimiento no consentido de aspectos de la vida privada) y de injerencias (acciones que buscan modificar la pauta de conducta desarrollada en la vida privada) lo que posibilita el libre desarrollo de la personalidad.

Procedimiento de disociación: la modificación de datos personales de manera que los detalles de las condiciones personales o materiales no puedan ya atribuirse a una persona identificada o identificable, o solo sea posible invirtiendo tiempo, costes y trabajo desproporcionado.

Protección de datos: Arrieta y Reusser, definen la protección de datos como "la protección jurídica que se otorga a las personas respecto de la recogida, almacenamiento, utilización, transmisión y cualquier otra operación realizada sobre sus respectivos datos, destinada a cuidar que su tratamiento se realice con lealtad y licitud, de manera que no afecte indebidamente sus derechos constitucionales, legales u otros de cualquier clase.

R)

Responsable de del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines, condiciones y medios del tratamiento de datos personales; en caso de que los fines, condiciones y medios del tratamiento estén determinados por 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; (Propuesta Reglamento 2012/0011 final)

Representante: toda persona física o jurídica establecida en la Unión que, designada expresamente por el responsable del tratamiento, actúe en lugar del responsable del tratamiento y a la que pueda dirigirse cualquier autoridad de control y otros organismos de la Unión en lugar del responsable del tratamiento, en lo que respecta a las obligaciones de este último en virtud del presente Reglamento; (Propuesta Reglamento 2012/0011 final)

Restricción del tratamiento: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro; (Propuesta Directiva COM 2012/0010 Final)

S)

Sede electrónica: es la dirección electrónica disponible para los ciudadanos a través de las redes de telecomunicaciones mediante la cual las administraciones públicas difunden información y prestan servicios.

Sistema de gestión de pasajeros PSS (Passenger Service System): es un conjunto de sistemas de gestión operativa y administrativa de las funciones de control de partidas, el inventario y el sistema de reservas.

Sistema de información Schengen (SIS): el Sistema de Información de Schengen o SIS es un sistema de información común que permite a las autoridades competentes de los Estados miembros disponer de información relativa a algunas categorías de personas y objetos**.**

Sistema de trasmisión (pull): método por el cual la autoridad requirente puede acceder al sistema de reservas de la compañía aérea y copiar los datos requeridos en su propia base de datos.

Sistema de transmisión (push): método por el cual las compañías aéreas transmiten los datos PNR requeridos a la base de datos de la autoridad requirente. Implica que la compañía aérea transmite los datos al tercer país y no que ésta permita el acceso del tercer país a sus bases de datos.

T)

Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, efectuadas o no sobre procedimientos automatizados, como la recogida, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, supresión o destrucción. (Propuesta COM 2012/0010 final). /(2) Se entenderá todo tratamiento o proceso de tratamientos relativo a datos de carácter personal, con o sin ayuda de procedimientos automatizados, tales como la recopilación, almacenamiento, organización, conservación, adaptación o modificación, lectura, consulta, utilización, la comunicación mediante transmisión, difusión o cualquier otra forma de puesta a disposición, la combinación o asociación, así como el bloqueo, cancelación o destrucción de datos; se considerará también tratamiento de datos de carácter personal a los efectos del presente Tratado la comunicación relativa a las existencia o inexistencia de una concordancia. (Tratado o Convenio de Prüm (Schengen III). Artículo 33 (1) 1.)

Tratamiento automatizado: se entiende las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: Registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión

V)

Vida privada: El derecho a la protección de la vida privada consiste en la facultad de las personas a mantener un ámbito de su vida fuera del conocimiento público, en el cual desarrolla acciones que se inician y concluyen en el sujeto que las realiza, como asimismo concreta relaciones francas, relajadas y cerradas que trascienden sólo a la familia o aquellos con los que determina compartir, siempre y cuando tales actuaciones y relaciones no dañen a otros, no sean delitos o no sean hechos de relevancia pública o que afecten al bien común. En el ámbito de privacidad e intimidad los terceros sólo pueden penetrar con el consentimiento de la persona afectada, poseyendo, asimismo, la persona la facultad de control de dichos actos, como asimismo, de los datos referentes a su vida privada e intimidad.

Violación de datos personales: toda violación de la seguridad que ocasione la destrucción accidental o ilícita, la pérdida, alteración, comunicación no autorizada o el acceso a datos personales transmitidos, conservados o tratados de otra forma;

Vuelo internacional: cualquier vuelo programado para entrar en el territorio de por lo menos un Estado miembro de la Unión Europea procedente de un tercer país o para salir del territorio de por lo menos un Estado miembro de la Unión Europea con destino final en un tercer país.

REFERENCIAS NORMATIVAS

I.- INTERNACIONAL

Carta de los Derechos Fundamentales de la Unión Europea. Publicado en el Diario Oficial de la Unión Europea con fecha 18 de diciembre de 2000.

Convención de Naciones Unidas sobre los Derechos del Niño, adoptada por la Asamblea General de las Naciones Unidas en su resolución 44/25, del 20 de noviembre de 1989.

Convenio de Roma, del Consejo de Europa, relativo a la salvaguarda de los derechos humanos y de las libertades fundamentales, del 4 de noviembre de 1950.

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

Declaración Universal de los Derechos Humanos, aprobada por la Asamblea General de las Naciones Unidas, del 10 de Diciembre de 1948.

Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales de la OCDE, de 23 de septiembre de 1980.

Pacto Internacional de Derechos Civiles y Políticos, adoptado y abierto para su firma, ratificación y adhesión por la Asamblea General de las Naciones Unidas a contar del 16 de diciembre de 1966.

Protocolo Adicional de Convenio nº 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos, de 8 de noviembre de 2001.

Recomendación nº R (87) 15, del Consejo de Europa, que regula la utilización de datos personales en el sector de la policía, de 17 de septiembre 1987.

Resolución nº 2.450 de la Asamblea General de Naciones Unidas, sobre Derecho y Progreso de la Ciencia y Técnica, de 19 de Diciembre de 1968.

Resolución 45/1995 de la Asamblea General de Naciones Unidas, por la que se establecen las directrices de protección de datos, de 14 de diciembre de 1990.

Resolución de Madrid sobre estándares internacionales sobre protección de datos personales y privacidad, adoptada por la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada el 5 de noviembre de 2009.

II.- UNIÓN EUROPEA

Acuerdo de Schengen de 14 de junio de 1985, relativo a la supresión gradual de controles en las fronteras comunes.

Convenio de aplicación del Acuerdo de Schengen de 19 de junio 1990, entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa, relativo a la supresión gradual de los controles en las fronteras comunes.

Decisión 1999/C 26/06 del Consejo de 3 de diciembre de 1998 por la que se encomienda a Europol la lucha contra los delitos cometidos o que puedan cometerse en el marco de actividades terroristas que atenten contra la vida, la integridad física, la libertad o los bienes de las personas.

Decisión 2000/520/CE de la Comisión de 26 de julio de 2000, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.

Decisión 2001/C 362/01 del Consejo de 6 de diciembre de 2001 por la que se amplían las competencias de Europol a las formas graves de delincuencia internacional enumeradas en el anexo del Convenio Europol.

Decisión 2001/497/CE de 15 de junio de 2001, de la Comisión, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE de 24 octubre 1995, del Parlamento Europeo y del Consejo.

Decisión 2002/2/CE de 20 de diciembre de 2001, de la Comisión, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense «*Personal Information and Electronic Documents Act*».

Decisión 2002/16/CE de 27 de diciembre de 2001, de la Comisión, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE de 24 octubre 1995, del Parlamento Europeo y del Consejo.

Decisión 2002/187/JAI del Consejo de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia.

Decisión 2002/494/JAI del Consejo de 13 de junio de 2002, relativa a la creación de una red europea de puntos de contacto en relación con personas responsables de genocidio, crímenes contra la humanidad y crímenes de guerra.

Decisión 2002/996/JAI del Consejo de 28 de noviembre de 2002, por la que se establece un mecanismo de evaluación de los sistemas legales y su ejecución a escala nacional en la lucha contra el terrorismo.

Decisión 2003/170/JAI del Consejo de 27 de febrero de 2003, relativa al uso conjunto de los funcionarios de enlace destinados en el extranjero por parte de los servicios policiales de los Estados miembros.

Decisión 2003/490/CE de la Comisión de 30 de junio de 2003, que aplica la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina.

Decisión 2003/659/JAI del Consejo de 29 de septiembre de 2003, por la que se modifica la Decisión 2002/187/JAI por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia.

Decisión 2003/821/CE de la Comisión de 21 de noviembre de 2003, relativa al carácter adecuado de la protección de los datos personales en Guernsey.

Decisión 2004/411/CE de la Comisión de 28 de abril de 2004, relativa al carácter adecuado de la protección de los datos personales en la Isla de Man.

Decisión 2004/452/CE de la Comisión de 29 de abril de 2004, por la que se establece una lista de organismos cuyos investigadores pueden acceder, con fines científicos, a datos confidenciales.

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

Decisión 2004/512/CE del Consejo de 8 de junio de 2004, por la que se establece el Sistema de Información de Visados (VIS).

Decisión 2004/535/CE de la Comisión de 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (*Bureau of Customs and Border Protection*).

Decisión 2004/644/CE del Consejo de 13 de septiembre de 2004, por la que se adoptan las normas de desarrollo del Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

Decisión 2004/915/CE de la Comisión, de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países.

Decisión 2005/267/CE del Consejo de 16 de Marzo de 2005, por la que se crea en Internet una red segura de información y coordinación para los servicios de gestión de migración de los Estados miembros.

Decisión 2005/681/JAI de 20 de septiembre de 2005, por la que se crea la Escuela Europea de Policía (CEPOL) y por la que se deroga la Decisión 2000/820/JAI.

Decisión 2006/253/CE de la Comisión de 6 de septiembre de 2005, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros (*Passenger Name Records*, PNR) que se transfieren a la *Canada Border Services Agency* (Agencia de Servicios de Fronteras de Canadá) y Anexo, con los compromisos por la Agencia Canadiense de Servicios Fronterizos en relación con la aplicación de su Programa de PNR.

Decisión 2006/230/CE del Consejo de 18 de julio de 2005, relativa a la celebración de un Acuerdo entre la Comunidad Europea y el Gobierno de Canadá sobre el tratamiento de datos API/PNR

Decisión 2006/648/CE de la Comisión de 22 de septiembre de 2006, por la que se establecen las especificaciones técnicas de las normas sobre los identificadores biométricos en relación con el Sistema de Información de Visados.

Decisión 2006/729/PESC/JAI del Consejo de 16 de octubre de 2006, relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos.

Decisión 2006/752/CE de la Comisión de 3 de noviembre de 2006, por la que se determinan las localizaciones del Sistema de Información de Visados durante la fase de desarrollo

Decisión 2007/124/CE del Consejo de 12 de febrero de 2007, por la que se establece para el período 2007-2013 el programa específico Prevención, preparación y gestión de las consecuencias del terrorismo y de otros riesgos en materia de seguridad, integrado en el programa general Seguridad y defensa de las libertades

Decisión 2007/125/JAI del Consejo de 12 de febrero de 2007, por la que se establece para el período 2007-2013 el programa específico Prevención y lucha contra la delincuencia, integrado en el programa general Seguridad y defensa de las libertades.

Decisión 2007/170/CE de la Comisión de 16 de marzo de 2007, por la que se establecen los requisitos de la red para el Sistema de Información de Schengen II (primer pilar).

Decisión 2007/171/CE: de la Comisión de 16 de marzo de 2007, por la que se establecen los requisitos de la red para el Sistema de Información de Schengen II (tercer pilar).

Decisión 2007/533/JAI del Consejo de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II).

Decisión 2007/551/PESC/JAI del Consejo de 23 de julio de 2007, relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y los Estados Unidos de América, sobre el tratamiento y la transferencia de datos del registro de

nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos.

Decisión 2008/49/CE de la Comisión de 12 de diciembre de 2007, relativa a la protección de los datos personales en la explotación del Sistema de Información del Mercado Interior (IMI).

Decisión 2008/173/CE del Consejo, de 18 de febrero de 2008, relativa a los ensayos del Sistema de Información de Schengen de segunda generación (SIS II)

Decisión 2008/333/CE de la Comisión de 4 de marzo de 2008, por la que se adopta el Manual Sirene y otras medidas de ejecución para el Sistema de Información de Schengen de segunda generación (SIS II).

Decisión 2008/334/JAI de la Comisión de 4 de marzo de 2008, por la que se adopta el Manual Sirene y otras medidas de ejecución para el Sistema de Información de Schengen de segunda generación (SIS II)

Decisión 2008/597/CE de la Comisión de 3 de junio de 2008, por la que se adoptan disposiciones de aplicación relativas al Responsable de la Protección de Datos de conformidad con el artículo 24, apartado 8, del Reglamento (CE) nº 45/2001 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

Decisión 2008/602/CE de la Comisión de 17 de junio de 2008, por la que se establecen la arquitectura física y las características de las interfaces nacionales y de la infraestructura de comunicación entre el Sistema Central de Información de Visados y las interfaces nacionales para la fase de desarrollo.

Decisión 2008/615/JAI del Consejo de 23 de Junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza.

Decisión 2008/616/JAI del Consejo de 23 de Junio de 2008, relativa a la ejecución de la Decisión 2008/615/JAI sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza.

Decisión 2008/617/JAI del Consejo de 23 de junio de 2008, sobre la mejora de la cooperación entre las unidades especiales de intervención de los Estados miembros de la Unión Europea en situaciones de crisis.

Decisión 2008/651/PESC/JAI del Consejo de 30 de junio de 2008, relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y Australia sobre el tratamiento y la transferencia de datos, generados en la Unión Europea, del registro de nombres de los pasajeros (PNR) por las compañías aéreas a los Servicios de Aduanas de Australia.

Decisión 2008/679/JAI de la Comisión de 31 de julio de 2008, relativa a la concesión de subvenciones para traducir y ensayar un módulo de encuesta de victimización con

arreglo al programa específico «Prevención y lucha contra la delincuencia» integrado en el programa general «Seguridad y defensa de las libertades».

Decisión 2009/316/JAI del Consejo de 6 de abril de 2009, por la que se establece el Sistema Europeo de Información de Antecedentes Penales (ECRIS) en aplicación del artículo 11 de la Decisión Marco 2009/315/JAI.

Decisión 2009/371/JAI del Consejo de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (Europol)

Decisión 2009/426/JAI del Consejo de 16 de diciembre de 2008, por la que se refuerza Eurojust y se modifica la Decisión 2002/187/JAI por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia

Decisión 2009/746/CE de la Comisión de 9 de octubre de 2009, por la que se establecen especificaciones sobre la resolución y el uso de impresiones dactilares a efectos de la verificación e identificación biométricas en el Sistema de Información de Visados.

Decisión 2009/876/CE de la Comisión de 30 de noviembre de 2009, por la que se adoptan medidas técnicas de aplicación para introducir los datos y las solicitudes vinculados entre sí, acceder a los datos, modificar, suprimir y suprimir anticipadamente datos, conservar registros de operaciones de tratamiento de datos y acceder a ellos en el Sistema de Información de Visados.

Decisión 2009/934/JAI del Consejo de 30 de noviembre de 2009, por la que se adoptan las normas de desarrollo que rigen las relaciones de Europol con los socios, incluido el intercambio de datos personales y de información clasificada

Decisión 2009/935/JAI del Consejo de 30 de noviembre de 2009, por la que se determina la lista de terceros Estados y organizaciones con los que Europol celebrará acuerdos

Decisión 2009/936/JAI del Consejo de 30 de noviembre de 2009, por la que se adoptan las normas de desarrollo aplicables a los ficheros de trabajo de análisis de Europol

Decisión 2009/968/JAI del Consejo de 30 de noviembre de 2009, por la que se adoptan las normas sobre confidencialidad de la información de Europol

Decisión 2009/1010/JAI del Consejo de Administración de Europol de 4 de junio de 2009, sobre las condiciones relativas al tratamiento de datos en virtud del artículo 10, apartado 4, de la Decisión Europol.

Decisión 2009/1023/JAI del Consejo de 21 de septiembre de 2009, relativa a la firma, en nombre de la Unión Europea, y a la aplicación provisional de determinadas disposiciones del Acuerdo entre la Unión Europea, Islandia y Noruega para la aplicación de determinadas disposiciones de la Decisión 2008/615/JAI del Consejo sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, y de la Decisión 2008/616/JAI del Consejo relativa a la ejecución de la Decisión 2008/615/JAI sobre la

profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, y de su anexo.

Decisión 2010/49/CE de la Comisión de 30 de noviembre de 2009, por la que se determinan las primeras regiones para la puesta en marcha del Sistema de Información de Visados (VIS).

Decisión 2010/87/CE 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.

Decisión 2010/146/UE de la Comisión de 5 de marzo de 2010, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada dada en la Ley de las Islas Feroe sobre el tratamiento de datos personales

Decisión 2010/260/UE de la Comisión de 4 de mayo de 2010, relativa al plan de seguridad para el funcionamiento del Sistema de Información de Visados

Decisión 2010/261/UE de la Comisión de 4 de mayo de 2010, relativa al plan de seguridad para el SIS II Central y la infraestructura de comunicación

Decisión 2010/625/UE de la Comisión de 19 de octubre de 2010, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la adecuada protección de los datos personales en Andorra

Decisión 2010/689/UE del Consejo de 8 de noviembre de 2010, relativa al establecimiento del intercambio automatizado de datos respecto a los datos del ADN en Eslovaquia.

Decisión 2011/61/CE de la Comisión de 31 de enero de 2011, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por el Estado de Israel en lo que respecta al tratamiento automatizado de los datos personales.

Decisión 2011/355/UE del Consejo de 9 de junio de 2011, relativa al establecimiento del intercambio automatizado de datos dactiloscópicos en Francia

Decisión 2011/387/UE del Consejo de 28 de junio de 2011, relativa al establecimiento de un intercambio automatizado de datos por lo que respecta a los datos de matriculación de vehículos (DMV) en Eslovenia

Decisión 2011/434/UE del Consejo de 19 de julio de 2011, relativa al establecimiento del intercambio automatizado de datos dactiloscópicos en la República Checa.

Decisión 2011/547/UE del Consejo de 12 de septiembre de 2011, relativa al establecimiento de un intercambio automatizado de datos por lo que respecta a los datos de matriculación de vehículos (DMV) en Rumania.

Decisión 2012/236/UE del Consejo de 26 de abril de 2012, relativa al establecimiento de un intercambio automatizado de datos por lo que respecta a los datos de matriculación de vehículos (DMV) en Polonia.

Decisión 2012/664/UE del Consejo de 25 de octubre de 2012, relativa al establecimiento de un intercambio automatizado de datos por lo que respecta a los datos de matriculación de vehículos (DMV) en Suecia.

Decisión 2012/713/UE del Consejo de 13 de noviembre de 2012, relativa al establecimiento de un intercambio automatizado de datos por lo que respecta a los datos de matriculación de vehículos (DMV) en Lituania.

Decisión 2013/392/UE del Consejo de 22 de julio de 2013, por la que se establece la fecha a partir de la cual surtirá efecto la Decisión 2008/633/JAI sobre el acceso para consultar el Sistema de Información de Visados (VIS) por las autoridades designadas de los Estados miembros y por Europol, con fines de prevención, detección e investigación de delitos de terrorismo y otros delitos graves.

Decisión de Ejecución 2012/233/UE de la Comisión de 27 de abril de 2012, por la que se fija la fecha de puesta en marcha en una segunda región del Sistema de Información de Visados (VIS)

Decisión de Ejecución 2012/274/UE de la Comisión de 24 de abril de 2012, por la que se determina el segundo grupo de regiones para la puesta en marcha del Sistema de Información de Visados (VIS)

Decisión de Ejecución 2012/512/UE de la Comisión de 21 de septiembre de 2012, por la que se fija la fecha en que el Sistema de Información de Visados (VIS) se pondrá en marcha en una tercera región

Decisión de Ejecución 2013/266/UE de la Comisión de 5 de junio de 2013, por la que se fija la fecha de entrada en funcionamiento del Sistema de Información de Visados (VIS) en una sexta y una séptima región.

Decisión Marco 2005/222/JAI del Consejo de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información

Decisión Marco 2006/960/JAI del Consejo de 18 de diciembre de 2006, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea.

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

Decisión Marco 2009/948/JAI del Consejo de 30 de noviembre de 2009, sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales.

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

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

Directiva 2002/22/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas.

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 2004/82/CE del Consejo de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas.

Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores.

Directiva 2012/13/UE del Parlamento Europeo y del Consejo de 22 de mayo de 2012, relativa al derecho a la información en los procesos penales.

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

Propuesta de Decisión marco, COM (2007) 654 final, del Consejo de fecha 6 de noviembre de 2007, sobre utilización de datos del registro de nombres de los pasajeros (*Passenger Name Record* - PNR) con fines represivos.

Propuesta de Directiva COM(2012) 10 final, del Parlamento europeo y del Consejo, de fecha 25 de enero de 2012, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos.

Propuesta de Reglamento COM(2012) 11 final, del Parlamento y del Consejo, de fecha 25 de enero de 2012, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos).

Reglamento (CE) nº 2725/2000, del Consejo de 11 de Diciembre de 2000, relativo a la creación del sistema <<Eurodac>> para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín.

Reglamento 41/2001/CE, 18 de Diciembre de 2000, del Parlamento Europeo del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y organismos comunitarios y a la libre circulación de esos datos.

Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

Reglamento (CE) nº. 407/2002 del Consejo de 28 de Febrero de 2002, por el que se establecen determinadas normas de desarrollo del Reglamento (CE) nº 2725/2000 relativo a la creación del sistema <<Eurodac>> para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín.

Reglamento (CE) nº 831/2002 de la Comisión de 17 de mayo de 2002, por el que se aplica el Reglamento (CE) nº 322/97 del Consejo sobre la estadística comunitaria en lo relativo al acceso con fines científicos a datos confidenciales.

Reglamento (CE) n° 343/2003 del Consejo de 18 de febrero de 2003, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de asilo presentada en uno de los Estados miembros por un nacional de un tercer país.

Reglamento (CE) nº 1882/2003 del Parlamento Europeo y del Consejo de 29 de septiembre de 2003, sobre la adaptación a la Decisión 1999/468/CE del Consejo de las disposiciones relativas a los comités que asisten a la Comisión en el ejercicio de sus competencias de ejecución previstas en los actos sujetos al procedimiento establecido en el artículo 251 del Tratado CE.

Reglamento nº2007/2004 del Consejo de 26 de Octubre de 2004 por el que se crea una Agencia Europea para la gestión de la cooperación operativa en las fronteras exteriores de los Estados miembros de la Unión Europea.

Reglamento (CE) nº 2252/2004 del Consejo de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros.

Reglamento (CE) nº 1987/2006 del Parlamento Europeo y del Consejo de 20 de diciembre de 2006, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II).

Reglamento (CE) nº 81/2009 del Parlamento Europeo y del Consejo de 14 de enero de 2009, por el que se modifica el Reglamento (CE) nº 562/2006 en lo relativo al Sistema de Información de Visados (VIS) en el marco del Código de Fronteras Schengen.

Reglamento (CE) nº 544/2009 del Parlamento Europeo y del Consejo de 18 de junio de 2009, por el que se modifican el Reglamento (CE) nº 717/2007 relativo a la itinerancia en las redes públicas de telefonía móvil en la Comunidad y la Directiva 2002/2I/CE relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas.

Reglamento (UE) nº 1077/2011 del Parlamento Europeo y del Consejo de 25 de Octubre de 2011 por el que se establece una Agencia Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia.

Reglamento (UE) n° 1168/2011 del Parlamento Europeo y del Consejo de 25 de octubre de 2011, que modifica el Reglamento (CE) nº 2007/2004 del Consejo, por el que se crea una Agencia Europea para la gestión de la cooperación operativa en las fronteras exteriores de los Estados miembros de la Unión Europea.

Reglamento (UE) nº 977/2011 de la Comisión de 3 de octubre de 2011, que modifica el Reglamento (UE) nº 810/2009 por el que se establece el Código de Visados.

Reglamento (UE) nº 603/2013 del Parlamento Europeo y del Consejo de 26 de junio de 2013, relativo a la creación del sistema Eurodac para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (UE) nº 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley, y por el que se modifica el Reglamento (UE) nº 1077/2011, por el que se crea una Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia.

Reglamento (UE) nº 610/2013 del Parlamento Europeo y del Consejo de 26 de junio de 2013, por el que se modifica el Reglamento (CE) nº 562/2006 del Parlamento Europeo y del Consejo, por el que se establece un Código comunitario de normas para el cruce de personas por las fronteras (Código de fronteras Schengen), el Convenio de aplicación del Acuerdo de Schengen, los Reglamentos del Consejo (CE) nº 1683/95 y (CE) nº 539/2001 y los Reglamentos del Parlamento Europeo y del Consejo (CE) nº 767/2008 y (CE) nº 810/2009.

Tratado constitutivo de la Comunidad Europea de la Energía Atómica (EURATOM) en 1957

Tratado constitutivo de la Comunidad Europea (en la versión dada por el tratado de Maastricht de 7 de febrero de 1992 y el tratado de Ámsterdam de 2 de octubre de 1997) y modificado por el tratado de Niza firmado el día 26 de febrero de 2001 (Ley Orgánica

3/2001, de 6 de noviembre), por la que se autoriza la ratificación por España del tratado de Niza día 26 de febrero de 2001, modificado por acta de 23 de septiembre de 2003.

Tratado de Niza, de la Unión Europea firmado el 26 de Febrero de 2001, por el que se modifican el Tratado de la Unión Europea, los Tratados Constitutivos de las Comunidades Europeas y determinados actos conexos.

Tratado de Prüm, relativo a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal, de 27 de mayo de 2005, publicado en el BOE nº 307, de 25 de diciembre de 2006

Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea, firmado en Lisboa el 13 de diciembre de 2007.

III.- ESPAÑA

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

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

Real Decreto 1665/2008, de 17 de octubre, por el que se modifica el Estatuto de la Agencia Española de Protección de Datos, aprobado por Real Decreto 428/1993, de 26 de marzo.

Real Decreto 3/2010, de 8 de Enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de interoperabilidad en el ámbito de la Administración Electrónica

Real Decreto 203/2010, de 26 de febrero, por el que se aprueba el Reglamento de prevención
El Programa de la Haya: Consolidación de la Libertad, la Seguridad y la Justicia en la Unión Europea, (2005/C 53/01). Publicado en DOUE nº C 53/1 con fecha 3.3.2005

Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, por la que se crea el Registro Telemático de la Agencia Española de Protección de Datos.

Instrucción 2/1995, de 4 de mayo, de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal.

Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a edificios.

Instrucción 2/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo.

Instrucción 1/2004, de 22 diciembre de 2004, dc la Agencia Española de Protección de Datos, sobre publicación de sus Resoluciones.

Instrucción 1/2006, de 8 de Noviembre, de La Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

IV.- OTROS DOCUMENTOS

Carta de los EE.UU. a la UE, anexa al Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (Acuerdo PNR 2007). Publicada en el Diario Oficial de la UE nº L 204 de 4.8.2007

Comunicación COM(2010)385 final, de la Comisión al Consejo y al Parlamento Europeo, sobre el "Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia", de fecha 20.7.2010.

Comisión Europea, (DG XV D/5025/98, WP12), del Grupo de Trabajo del artículo 29, Documento de Trabajo, Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE. Aprobado por el Grupo de Trabajo el 24 de julio de 1998.

Compromiso de la Oficina de Aduanas y Protección Fronteriza del Departamento se Seguridad Nacional (CBP) en apoyo al Plan de la Comisión Europea para ejercer las facultades que le confiere el artículo 25 (6) de la Directiva 95/46/CE y adoptar una decisión de reconocer el Departamento de Seguridad Nacional de la Oficina de Aduanas y Protección Fronteriza (CBP) de proporcionar una protección adecuada a los efectos de las transferencias de las compañías aéreas de *Passenger Name Record* (PNR), que pueden estar dentro del ámbito de aplicación de la Directiva.

Dictamen 1/99, del Grupo de Trabajo del artículo 29, relativo al nivel de protección de datos en Estados Unidos y a los debates en curso entre la Comisión Europea y el Gobierno de Estados Unidos, 5092/98/ES/final WP 15, de 26 de enero de 1999.

Dictamen 10/2001, del Grupo de Trabajo del artículo 29, sobre la necesidad de un enfoque equilibrado en la lucha contra el terrorismo, de 14 de diciembre 2001.

Dictamen 4/2002 del Grupo de Trabajo del artículo 29, relativo al nivel de protección de datos personales en Argentina, de 3 de octubre de 2002.

Dictamen 6/2002 del Grupo de Trabajo del artículo 29, relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a los Estados Unidos, de fecha 24.10.2002

Dictamen 4/2003 del Grupo de Trabajo del artículo 29, relativo al nivel de protección garantizado en los EE.UU. para la transferencia de datos de pasajeros, de fecha 13.6.2003

Dictamen 1/2004 del Grupo de Trabajo del artículo 29, sobre el nivel de protección garantizado por Australia en la transmisión de datos del registro de nombres de pasajeros de las compañías aéreas, adoptado el 16 de enero de 2004.

Dictamen 3/2004 del Grupo de Trabajo del artículo 29, sobre el nivel de protección asegurado en Canadá para la transmisión de los Registros de Nombre de Pasajero (PNR) e Información Avanzada sobre Pasajeros (API) por parte de las aerolíneas (WP 88), adoptado el 11 de febrero de 2004

Dictamen 1/2005 del Grupo de Trabajo del artículo 29, sobre el nivel de protección garantizado por Canadá para la transmisión del PNR e información previa sobre pasajeros procedente de las compañías aéreas, aprobado por el Grupo el 19 de enero de 2005

Dictamen 2/2007 del Grupo de Trabajo del artículo 29, relativo a la información de los pasajeros en relación con la transferencia de datos PNR a las autoridades de los Estados Unidos. Emitido el 15 de febrero de 2007 y revisado y actualizado el 24 de junio de 2008.

Dictamen 3/2010 del Grupo de Trabajo del artículo 29, sobre publicidad comportamental en línea, donde se encuentra el principio de responsabilidad.

Dictamen 1/2012 del Grupo de Trabajo del artículo 29, sobre propuestas de reforma de la protección de datos.

Dictamen 5/2007 del Supervisor Europeo de Protección de Datos, relativo al nuevo Acuerdo de la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por parte de las Compañías aérea del Departamento de Seguridad del Territorio Nacional de los Estados Unidos, celebrado en julio de 2007 adoptado el 17 de Agosto de 2007.

Segundo dictamen 2007/C 91/02 del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.

Tercer Dictamen 2007/C 139/01 del Supervisor Europeo de Protección de Datos sobre la propuesta de DM del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.

Dictamen 2007/C 169/02 del Supervisor Europeo de Protección de Datos sobre la iniciativa del Reino de Bélgica, la República de Bulgaria, la República Federal de Alemania, el Reino de España, la República Francesa, el Gran Ducado de Luxemburgo,

el Reino de los Países Bajos, la República de Austria, la República de Eslovenia, la República Eslovaca, la República Italiana, la República de Finlandia, la República Portuguesa, Rumanía y el Reino de Suecia con vistas a la adopción de la Decisión del Consejo sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza.

Dictamen 2007/C 255/02 del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión del Consejo por la que se crea la Oficina Europea de Policía (Europol) — COM (2006) 817 final.

Dictamen 2008/C 89/01 del Supervisor Europeo de Protección de Datos sobre la iniciativa de la República Federal de Alemania referida a una Decisión del Consejo relativa a la ejecución de la Decisión 2007/…/JAI sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza.

Dictamen 2008/C 101/01 del Supervisor Europeo de Protección de Datos sobre la propuesta de Directiva del Parlamento Europeo y del Consejo por la que se modifica, entre otras, 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 (Directiva sobre intimidad y comunicaciones electrónicas).

Dictamen 2008/C 110/01 del Supervisor Europeo de Protección de Datos acerca de la propuesta de Decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros (*Passenger Name Record*, PNR) con fines represivos.

Dictamen 2008/C 270/01 del Supervisor Europeo de Protección de Datos sobre la Decisión 2008/49/CE de la Comisión, de 12 de diciembre de 2007 , relativa a la protección de los datos personales en la explotación del Sistema de Información del Mercado Interior (IMI), por lo que se refiere a la protección de los datos personales.

Dictamen 2009/C 128/01 del Supervisor Europeo de Protección de Datos acerca del informe final del Grupo de Contacto de Alto Nivel entre la UE y Estados Unidos sobre el intercambio de información y la protección de la vida privada y los datos personales.

Dictamen 2011/C 181/01 del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones — Un enfoque global de la protección de los datos personales en la Unión Europea.

Dictamen 2011/C 181/02 del Supervisor Europeo de Protección de Datos sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves

Dictamen 2012/C 34/01 del Supervisor Europeo de Protección de Datos sobre la neutralidad de la red, la gestión del tráfico y la protección de la intimidad y los datos personales.

Informe de la Comisión al Parlamento europeo, al Consejo, al Comité Económico y Social europeo y al Comité de las Regiones. “Informe de 2012 sobre la aplicación de la Carta de los Derechos Fundamentales de la UE COM/2013/0271 final.”, de 8 de mayo de 2013.

Opinión del Abogado General, Pedro CRUZ VILLALÓN sobre los asuntos C‑293/12 y C-594/12, de fecha el 12 de diciembre de 2013.

Recomendación 1/2010 de la Agencia Catalana de Protección de Datos, sobre el encargado del tratamiento en la prestación de servicios por cuenta de entidades del sector público de Cataluña (Abril 2010).

Resumen 2012/C 336/05 del Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión Europea al Consejo y al Parlamento Europeo sobre la creación de un Centro Europeo de ciberdelincuencia

REFERENCIAS JURISPRUDENCIALES

I.- TRIBUNAL EUROPEO DE DERECHOS HUMANOS

Caso *Klass y otros v/s República Federal de Alemania,* de 6 de septiembre de 1978.

Caso *Dudgeon v/s The United Kingdom*, de 22 de octubre de 1981.

Caso *Leander v/s Sweden,* de 26 de marzo de 1987

Caso *Gaskin* v/s United Kingdom, de 7 de julio de 1989

Caso *Huvig*, de 24 de abril de 1990.

Caso *Guerra y otros v/s Italia*, de 19 de febrero de 1998

Caso *Bottav/s Italy*, de 24 de febrero de 1998.

Caso *Fressoz y Roire v/s Francia*, de 21 de enero de 1999

Caso *Rotaru v/s Rumania*, de 4 de mayo de 2000

Caso *Amann v/s Switzerland,* de 16 de febrero de 2000

Caso *Weber y Saravia v/s Alemania*, diciembre de 2000

Caso *N. F. vs. Italia*, de 2 de agosto de 2001.

Casos *I. y Goodwin vs. Reino Unido*, ambas de 11 de julio de 2002.

Caso *Odievre v/s France,* de 13 de febrero de 2003

Caso *S. y Marper c. Reino Unido*. Sentencia de 4 de diciembre de 2008.

Caso *Irlanda vs. Parlamento y Consejo,* de 29 de febrero de 2009.

II.- TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

Asunto C-151/00, *Comisión de las Comunidades Europeas contra República Francesa*, de 18 de enero de 2001.

Asuntos acumulados C-465/00, C-138/01 y C-139/01, *Rechnungshof (C-465/00) contra Österreichischer Rundfunk, y otros y entre Christa Neukomm (C-138/01), Joseph Lauermann (C-139/01) y Österreichischer Rundfunk,* de 20 de mayo de 2003.

Asunto C-101/01, *Göta hovrätt (Suecia) contra Bodil Lindqvist*, de 6 de noviembre de 2003.

Asunto C-350/02, *Comisión de las Comunidades Europeas contra Reino de los Países Bajos*, de 24 de junio de 2004.

Asunto C-376/04, *Comisión de las Comunidades Europeas contra Reino de Bélgica*, de 28 de abril de 2005

Asuntos acumulados C-317/04 y C-318/04, *Parlamento Europeo contra Consejo de la Unión Europea (C-317/04) y Comisión de las Comunidades Europeas (C-318/04)*, de 30 de mayo de 2006.

Asunto C-475/04, *Comisión de las Comunidades Europeas contra República Helénica*, de 1 junio 2006.

Asunto T-194/04, *The Bavarian Lager Co. Ltd contra Comisión de las Comunidades Europeas*, de 8 de noviembre de 2007.

Asuntos acumulados C-402/05 P y C-415/05 P, *Yassin Abdullah Kadi y Al Barakaat International Foundation contra Consejo de la Unión Europea y Comisión de las Comunidades Europeas*, de 3 de septiembre de 2008.

Asunto C‑524/06, *Heinz Huber contra Bundesrepublik Deutschland*, de 16 de diciembre de 2008

Asunto C-553/07, *College van burgemeester en wethouders van Rotterdam contra M. E. E. Rijkeboer*, de 7 de mayo de 2009.

Asunto C-518/07, *Comisión Europea contra República Federal de Alemania*, de 9 de marzo de 2010.

Asunto C-28/08 P, *Comisión Europea contra The Bavarian Lager Co. Ltd*., de 29 de junio de 2010.

Asunto C-343/09, *Afton Chemical Limited contra Secretary of State for Transport*, de 8 de julio de 2010.

Asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Schecke GbR (C-92/09) y Hartmut Eifert (C-93/09) contra Land Hessen*, de 9 de noviembre de 2010.

Asunto C-145/09, *Land Baden-Württemberg contra Panagiotis Tsakouridis*, de 23 de noviembre de 2010.

Asuntos acumulados C-468/10 y C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10)* y *Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) contra Administración del Estado*, de 24 de noviembre de 2011.

Asunto C-614/10, *Comisión Europea contra República de Austria*, de 16 de octubre de 2012.

Asuntos acumulados C-581/10 y C-629/10, *Emeka Nelson y otros contra Deutsche Lufthansa AG (C-581/10) y TUI Travel plc y otros contra Civil Aviation Authority (C-629/10)*, 23 de octubre de 2012.

Asuntos acumulados C-539/10 P y C-550/10 P, *Stichting Al-Aqsa contra Consejo de la Unión Europea* (C-539/10 P) *y Reino de los Países Bajos contra Stichting Al-Aqsa* (C-550/10 P), de 15 de noviembre de 2012.

Asunto C-119/12, *Josef Probst contra mr.nexnet GmbH*, de 22 de noviembre de 2012.

Asunto C-283/11, Sky Österreich GmbH contra Österreichischer Rundfunk, de 22 de enero de 2013.

Asunto C-101/12, Herbert Schaible contra Land Baden-Württemberg, de 17 de octubre de 2013.

Asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland* y *Seitlinger y otros*, de 8 de abril de 2014.

III.- TRIBUNAL CONSTITUCIONAL ESPAÑOL

Sentencia nº 254/1993 de 20 de julio. Recurso de amparo 1.827-1990.

Sentencia nº 143/1994 de 9 de mayo. Recurso de amparo 3.192-1992.

Sentencia nº 11/1998 de 13 de enero. Recurso de amparo 2.264-1996.

Sentencia nº 202/1999 de 8 de noviembre. Recurso de amparo 4.138-1996

Sentencia nº 290/2000 de 30 de noviembre. Recurso de inconstitucionalidad 201-93, 219-93, 226-93 y 236-93.

Sentencia nº 292/2000 de 30 de noviembre. Recurso de inconstitucionalidad 1463-2000.

Sentencia nº 203/2001 de 15 de octubre. Recurso de amparo 3900-1998, 3902-1998, 3903-1998 y 3904-1998 (acumulados).

Sentencia nº 85/2003 del 8 de mayo de 2003. Recurso de amparo electoral 2589-2003 y otros 376 (acumulados).

IV.- TRIBUNAL CONSTITUCIONAL ALEMÁN

Sentencia del Tribunal Constitucional Federal Alemán, sobre la Ley de Censo, de 15 de diciembre de 1983.

Sentencia del Tribunal Constitucional Federal Alemán, por la que se declara inconstitucional la norma que posibilitaba los registros *online* de los sistemas informáticos, de 27 de febrero de 2008.

RECURSOS DE INTERNET

I.- DIRECCIONES INSTITUCIONALES PÚBLICAS

Unión Europea

Página de la Unión Europea, http://europa.eu.int

Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales, http://europa.eu.int/comm/internal_market/fr/media/da_taprot/wpdocs/index.htm.

Supervisor Europeo de Protección de Datos, http://secure.edps.europa.eu/EDPSWEB/edps/EDPS?lang=es

Convención Europea, http://european-convention.eu.int/bienvenue.asp?lang=ES.

Consejo de Europa

Página del Consejo de Europa, http://www.coe.int/

Repertorio de jurisprudencia (HUDOC) del Tribunal Europeo de Derechos Humanos, http://www.echr.coe.int/Fr/Judgements.htm.

OCDE

Organización para la Cooperación y el Desarrollo Económicos, http://www.oecd.org/.

España

Agencia Española de Protección de Datos, http://www.agpd.es/portalwebAGPD/index-ides-idphp.php

Boletín Oficial del Estado, http://www.boe.es/aeboe/consultas/

II.- REVISTAS Y PUBLICACIONES ELECTRÓNICAS

Revista de Derecho Constitucional Europeo, http://www.ugr.es/~redce/ReDCEportada.htm

Biblioteca científica electrónica Dialnet, http://dialnet.unirioja.es/

Revista Catalana de Seguretat Pública, http://www.raco.cat/index.php/RCSP/index

Revista Española de Relaciones Internacionales, http://reri.difusionjuridica.es/index.php/RERI

Biblioteca de la Universidad de Alcalá, http://dspace.uah.es/dspace/handle/10017/391

European Integration online Papers, http://eiop.or.at/eiop/index.php/eiop/index

Asociación Profesional Española de Privacidad, http://www.apep.es/index.php

Librería de la Unión Europea, https://bookshop.europa.eu/es/home/

Revista de ciencias jurídicas y sociales FORO, Universidad Complutense de Madrid, http://revistas.ucm.es/index.php/FORO

Repertorio documental de la Universidad de Valladolid, http://uvadoc.uva.es

Red Iberoamericana de Protección de Datos, http://www.redipd.org/index-ides-idphp.php

Social Science Research Network, http://papers.ssrn.com/sol3/DisplayAbstractSearch.cfm

Revista para el Análisis del Derecho InDret, http://www.indret.com/es/

Fundación Coloquio Jurídico Europeo, http://www.fcje.org.es/

Depósito Digital de documentos de la Universidad Autónoma de Barcelona, http://ddd.uab.cat/

Cursos de Derecho Internacional y Relaciones Internacionales de Victoria-Gasteiz; Universidad del País Vasco, http://www.ehu.es/cursosderechointernacionalvitoria/inicio.htm

Repositorio Institucional de la Universidad de Huelva, http://rabida.uhu.es/dspace/

Base de datos jurídica V-lex, http://vlex.com/

Base de datos jurídicos westlaw, http://westlaw.es/wles/app/search/template?tid=universal

Base de datos jurídicos la ley digital, http://laleydigitalhome.laley.es/content/Inicio.aspx

Base de datos jurídicos Tirant lo Blanch, http://www.tirantonline.com/index.do

Base de datos jurídicos, jurisprudencia y doctrina, especialmente de Canadá, Estados Unidos y la Unión Europea Lexisnexis, http://www.lexisnexis.es/

Centro de Documentación Europea, Universidad de Alicante, http://www.cde.ua.es/

Revista fallos del mes, http://www.fallosdelmes.cl/revista.html

Catálogo de publicaciones, Universidad de Bologna, http://spogli.cib.unibo.it/cgi-ser/start/it/spogli/ds-s.tcl?fasc_issn=0716-1883&data_ins=Tutti

Catálogo de Biblioteca científica online, Scielo, http://www.scielo.cl/

Revista chilena de Derecho, Pontificia Universidad Católica de Chile, *http://derecho.uc.cl/publicaciones/revista-chilena-de-derecho/*

Revista de Derecho, Universidad Austral de Chile, *http://www.derecho.uach.cl/investigacion/revista-derecho.php*

Boletines Europeos, Universidad Castilla la Mancha, *http://pagina.jccm.es/europa/asuntoseurop.htm*

Consorcio para el acceso a la información científica electrónica, CINCEL, *http://www.cincel.cl/content/view/388/1/*

BIBLIOGRAFÍA

ACED FÉLEZ, Emilio. "Ejercicio y garantía del derecho a la protección de datos personales en el Convenio de Prüm". *Revista de derecho constitucional europeo*, nº 7, (2007): 65-96.

— "La protección de datos en la cooperación policial europea: de la Recomendación (87) 15 al principio de disponibilidad: Título IV. Disposiciones Sectoriales. Cap. I. Ficheros de Titularidad Pública. Artículos 22, 23.1 y 24.1". En *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, 1350-1388. Accedido 11 de abril de 2013. http://dialnet.unirioja.es/servlet/articulo?codigo=3693923.

— "Principio de disponibilidad y protección de datos en el ámbito policial". Noticias Jurídicas, 2010. http://noticias.juridicas.com/articulos/15-Derecho%20Administrativo/201004-123095321697634.html.

ACOSTA GALLO, Pablo. "La evolución hacia una Administración europea de los asuntos de Libertad, Seguridad y Justicia". *Revista CIDOB d'afers internacionals,* nº 91, (2010): 105-123.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. "El Derecho Fundamental a la Protección de Datos: Guía para el Ciudadano". Accedido 12 de agosto de 2013. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_CIUDADANO_OK.pdf.

ALBRECHT, Jan Philipp. "Por una Europa de los derechos ciudadanos". La promoción del 2009 (s. f.): 13 y ss.

ALDECOA LUZÁRRAGA, Francisco, y Mercedes GUINEA LLORENTE. *La Europa que viene: el Tratado de Lisboa*. 2° ed. Madrid: Marcial Pons, 2010.

ALLEN, A.L. "Privacy as data control: conceptual, practical and moral limits of the paradigm". *Connecticut Law Review* nº 32 (2000): 861-875.

ALONSO MOREDA, Nicolás. "Eurojust, a la vanguardia de la cooperación judicial en materia penal en la Unión Europea". *Revista de Derecho Comunitario Europeo* Año nº 16, Nº 41 (2012): 119-157.

ALPA, Guido. "Novissimo digesto italiano" 15 (1982).

— Privacy e statuto dell'informazione. banche dati, telemática e diritti della persona, 1984.

ÁLVARES VÉLIZ, María I, y María F ALCÓN YUSTAS. *Las constituciones de los quince Estados de la Unión Europea: Textos y comentarios*. Madrid: Dykinson, 1996.

ÁLVAREZ-CIENFUEGOS SUÁREZ, José María. *La defensa de la intimidad de los ciudadanos y la tecnología informática.* Aranzadi, 1999.

AMEZÚA AMEZÚA, Luis Carlos. *Los derechos fundamentales en la Unión Europea.* Accedido 12 de agosto de 2013. http://dialnet.unirioja.es/servlet/articulo?codigo=2308341.

AMOEDO SOUTO, Carlos Alberto. "La cooperación policial en la Unión Europea: su repercusión en el modelo español de seguridad pública". *Revista Catalana de Seguretat Pública*, nº17, 2006. 46-60

ANDERSSON, Rubén. "Frontex y la creación de la frontera euroafricana: golpeando la valla ilusoria". *Revista de derecho migratorio y extranjería*, n° 28 (2011): 177-191.

ANDRÉS SÁENZ DE SANTA MARÍA, Paz. "El sistema institucional en el Tratado de Lisboa: entre la continuidad y el cambio". *En El Tratado de Lisboa: la salida de la crisis constitucional: Jornadas de la Asociación Española de Profesores de Derecho Internacional-AEPDIRI-celebradas en Madrid el 17 y 18 de diciembre de 2007*, 205-225. Iustel, 2008.

ANGUITA OLMEDO, Concepción. "La delincuencia organizada: un asunto interior de la unión europea. Concepto, características e instrumentos para su neutralización". *Revista Española de Relaciones Internacionales*, nº 2, (2010): 152-172.

ANGUITA RAMÍREZ, Pedro. *La protección de datos personales y el derecho a la vida privada. Régimen jurídico, jurisprudencia y derecho comparado*. Santiago de Chile: Editorial Jurídica de Chile, 2007.

APARICIO SALOM, Javier. *Estudio sobre la ley orgánica de protección de datos de carácter personal*. 3º edición. Pamplona: Aranzadi, 2009.

APRELL LASAGABASTER, María de la Concepción. "Hacia la creación del espacio común europeo: La política de visados de la Unión Europea". En *Persona y Estado en el umbral del siglo XXI*, editado por Ana Salinas de Frías, 41-48. Málaga: Universidad de Málaga (UMA), Facultad de Derecho, 2001.

ARENAS GARCÍA, Rafael y PÉREZ FRANCESCH, Joan Lluís, "Extranjería (II) entrada en el espacio Schengen y permanencia en España", en *Tratado de Derecho de la Persona Física*, Mª del Carmen GETE-ALONSO Y CALERA y Judith SOLÉ RESINA (Coords.), Vol. 2, Cívitas, Navarra, 2013, pp. 467-536.

ARENAS RAMIRO, Mónica. "El derecho a la protección de datos personales: de la jurisprudencia del TEDH a la del TJCE". En *Constitución y democracia: 25 años de Constitución democrática en España: (actas del congreso celebrado en Bilbao los días 19 a 21 de noviembre de 2003)*, editado por Miguel A. GARCÍA HERRERA, 575-588. Bilbao: Servicio Editorial de la Universidad del País Vasco, 2005.

— *El derecho fundamental a la protección de datos personales en Europa*. Valencia: Tirant lo Blanch, 2006.

— "Integración europea y protección de datos personales. Las garantías específicas del derecho a la protección de datos personales". *Anuario de la Facultad de Derecho de 2004*, Universidad de Alcalá de Henares 2005. 7-45.

— "La protección de datos personales en los países de la Unión Europea". *Revista jurídica de Castilla y León* nº 16 (2008): 113-168.

ARIAS RODRÍGUEZ, José Manuel. "El Programa de Estocolmo". *Diario La Ley* nº 7812 (2012): 2 y ss.

ARRIETA CORTÉS, Raúl (Cord.), *Reflexiones Sobre el Uso y Abuso de los Datos Personales en Chile*, Expansiva, Santiago de Chile, 2011

ARRIETA CORTÉS, Raúl, y Carlos REUSSER MONSÁLVEZ. *Chile y la protección de datos personales ¿están en crisis nuestros derechos fundamentales?*. Santiago de Chile: Universidad Diego Portales, 2009.

ARROYO ROMERO, Francisco Javier. "La influencia de Europol en la comunitarización de la policía europea". Madrid: Akal, 2005.

ARZOZ SANTIESTEBAN, Xabier. "Artículo 8: derecho al respeto de la vida privada y familiar". En *Convenio Europeo de Derechos Humanos. Comentario sistemático*, editado por Iñaki LASAGABASTER HERRARTE. Navarra: Thomson-Reuters Civitas, 2009.

AUS, Jonathan P. "Eurodac: A Solution Looking for a Problem?" *European integration online papers* (EIoP) Nº 10 (21 de julio de 2006): 1-26.

AYALA, José Enrique. "Lisboa, por fin: el tratado abre una nueva era en la UE". *Política exterior* 24, nº 133 (2010): 13-20.

BALADO RUÍZ-GALLEGOS, Manuel, José Antonio GARCÍA REGUEIRO, y María José DE LA FUENTE y DE LA CALLE, eds. *La declaración universal de los derechos humanos en su 50 aniversario*. Barcelona: Bosch, 1998.

BALDASSARRE, Antonio. *Privacy e contituzione. L' esperienza statunitense*. Roma: Bulsuni, 1974.

BARCELÓ, Rosa y PÉREZ ASINARI, María Verónica, «Transferencia internacional de datos personales», en *Protección de Datos: Comentarios a la LOPD y su Reglamento de Desarrollo*, Tirant lo blanch, Valencia, 2009.

BATLLÉ SALES, Georgina. *El derecho a la intimidad privada y su regulación*. Alcoy: Marfil, 1972.

BAYO DELGADO, Joaquín. "Derecho comunitario sobre protección de datos". *Cuadernos de derecho judicial* n° 9 (2004): 45-75.

— "La cooperación policial internacional a la luz de la Propuesta revisada de Decisión Marco relativa a la protección de datos". En *La protección de datos en la cooperación policial y judicial. Pamplona*: Aranzadi, 2008. 21-36

— "La protección de datos en el ámbito judicial". *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid* n° 50 (2011).

— "La protección de datos en la investigación policial y en el proceso penal". *Jueces para la democracia* n° 63 (2008): 11-24.

BECERRIL ATIENZA, Belén. "La regulación de la cooperación reforzada y su reforma en Lisboa: hacia un modelo de diferenciación más cercano al método comunitario". En *Unidad y flexibilidad en el futuro de la Unión Europea: el desafío de las cooperaciones reforzadas*, 15-34. Universidad San Pablo-CEU, 2010.

BÉJAR MERINO, Helena. "Autonomía y dependencia: la tensión de la intimidad". *Revista española de investigaciones sociológicas* (1987): 69-89.

— "La génesis de la privacidad en el pensamiento liberal". *Sistema: revista de ciencias sociales* (1987): 59-72.

BENDA, Ernst. "Dignidad humana y derechos de la personalidad". En *Manual de Derecho Constitucional*, traducido por Antonio LÓPEZ PINA. Madrid: Marcial Pons, 1996.

BENEYTO PÉREZ, José María, Jerónimo MAILLO GONZÁLEZ-ORÚS, y Belén BECERRIL ATIENZA, eds. *Unidad y flexibilidad en el futuro de la Unión Europea: el desafío de las cooperaciones reforzadas*. Instituto Universitario de Estudios Europeos de la Universidad San Pablo-CEU, 2010.

BERMEJO CASADO, Rut. "El proceso de institucionalización de la cooperación en la gestión operativa de las fronteras externas de la UE: La creación de Frontex". *Revista CIDOB d'afers internacionals* nº 91 (2010): 29-62.

BIGLINO CAMPOS, M. Paloma. "De qué hablamos en Europa cuando hablamos de Derechos fundamentales: el argumento de Hamilton". *Revista de Derecho Comunitario Europeo* nº 14 (2003): 45-68.

BLAS, Frédéric. "Transferencias Internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales". *Revista Derecho del Estado* nº 23 (diciembre de 2009): 37-66.

BLASI CASAGRAN, Cristina. "La protección de los Derechos Fundamentales en el Tratado de Lisboa". *Institut Universitari d' Estudis Europeus 51. Quaderns de treball* (octubre de 2010): 1-68.

BLOUSTEIN, Edward J. "Privacy as an aspect of human dignity: an answer to Dean PROSSER,". *New York University Law Rewiew* vol. 39 (diciembre de 1964): 964-1007.

BORCHARDT, Klaus-Dieter. *El ABC del Derecho de la Unión Europea*. Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2011. http://bookshop.europa.eu/is-bin/INTERSHOP.enfinity/WFS/EU-Bookshop-Site/es_ES/-/EUR/ViewPublication-Start?PublicationKey=OA8107147.

BRADY, Hugo. "Europol y el Modelo europeo de inteligencia criminal: una respuesta no estatal a la delincuencia organizada". *Análisis del Real Instituto Elcano (ARI)* nº 126 (2007): 1-7.

BRAGE CAMEZANO, Joaquín. "Aproximación a una teoría general de los derechos fundamentales en el Convenio Europeo de Derechos Humanos". *Revista Española de Derecho Constitucional* nº 74 (2005): 111-138.

BRÉVILLE, Benoît. "Inmigración selectiva a la estadounidense: en un futuro próximo, ¿se subastarán los visados?" *Le Monde diplomatique en español*. n° 212. Junio de 2013.

CABEZUDO BAJO, María José. "El régimen de protección del dato de ADN en la Unión Europea y en España: planteamiento de la cuestión". En *Los retos del Poder Judicial ante la sociedad globalizada. Actas del IV Congreso Gallego de Derecho Procesal (I Internacional) A Coruña, 2 y 3 de junio de 2011,* Agustín Jesús Pérez-Cruz Martín y Xulio Ferreiro Baamonde (dirs.). Editorial Universidad da Coruña (2012): 307-318.

— "La protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal". En *La justicia y la carta de derechos fundamentales de la Unión Europea.* Editorial Constitución y Leyes, COLEX (2008): 327-342.

— "La protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal". http://www.oesd.org/?p=167#more-167.

CALDUCH CERVERA, Rafael. *Relaciones Internacionales*. Ediciones Ciencias Sociales. Madrid, España, 1991.

CALLEJÓN, Francisco Balaguer. "El Tratado de Lisboa en el diván. Una reflexión sobre estatalidad, constitucionalidad y Unión Europea". *Revista española de derecho constitucional*, nº 83 (2008): 57-92.

CÁMARA VILLAR, Gregorio. "La garantía de los derechos fundamentales afectados por la Convención de Prüm". *Revista de derecho constitucional europeo* nº 7 (2007): 97-118.

CAO AVELLANEDA, Javier. "Big data y LOPD, ¿Enemigos íntimos?. *Apuntes de seguridad de la información*. http://seguridad-de-la-informacion.blogspot.com.es/2012/12/big-data-y-lopd-enemigos-intimos.html.

CARRERAS SERRA, Lluis de. *Régimen jurídico de la información. Periodistas y medios de comunicación*. Barcelona: Ariel, 1996.

CARRILLO LÓPEZ, Marc. *El derecho a no ser molestado: información y vida privada*. Pamplona: Thompson-Aranzadi, 2003.

CARRILLO SALCEDO, Juan Antonio. *Dignidad frente a barbarie: la Declaración Universal de Derechos Humanos cincuenta años después*. Madrid: Trotta, 1999.

— *El Convenio Europeo de Derechos Humanos*, Madrid, Tecnos, 2004.

— "Notas sobre el significado político y jurídico de la Carta de los Derechos Fundamentales de la Unión Europea". *Revista de Derecho Comunitario Europeo* nº 9 (2001): 7-26.

CARUSO FONTÁN, Viviana. "Bases de datos policiales sobre identificadores obtenidos a partir del ADN y derecho a la intimidad genética". *FORO. Revista de Ciencias Jurídicas y Sociales*, Nueva Época 15, nº 1 (2012): 135-167.

CASTAÑO SUÁREZ, Raquel. "Directiva 95/46, 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: Similitudes y diferencias con la Ley Orgánica 5/1992, de 29 de octubre (LORTAD)". *Noticias de la Unión Europea* n° 162 (1998): 9-16.

CATE, Fred H. "Personal information in Financial Service". *Financial Services Coordinating Council* (2000).

— "Principles on Internet Privacy". *Connecticut Law Review* (2000): 877-896.

CATILLEJO MANZANARES, Raquel. "Europol y las investigaciones transfronterizas". En *Piratas, mercenarios, soldados, jueces y policías: nuevos desafíos del derecho penal europeo e internacional*, de Luis Alberto Arroyo Zapatero, Adán Nieto Martín, Marta Muñoz de Morales Romero, y Matías Bailome. Cuenca: Universidad de Castilla-La Mancha, 2010.

— "EUROPOL y las investigaciones transfronterizas". *Dereito: Revista jurídica da Universidad de Santiago de Compostela* Vol. 17, Nº 2 (2008): 91-104.

CHICHARRO LÁZARO, Alicia. "El Tratado de Lisboa y el programa de Estocolmo: Los nuevos retos de la cooperación judicial en materia civil". *Revista electrónica de estudios internacionales* nº 20 (2010): 4-ss.

CHUECA SANCHO, Ángel Gregorio. "Por una Europa de los derechos humanos: la adhesión de la Unión Europea al Convenio Europeo de Derechos Humanos". En *Unión Europea y Derechos fundamentales en perspectiva constitucional*, editado por N. FERNÁNDEZ SOLA, 37-58. Madrid: Dykinson, 2004.

CLARO QUINTÁNS, Irene. "El sistema 'Eurodac' y la identificación de los solicitantes de asilo en la Unión Europea". En *El día de Europa: las transformaciones de la Unión Europea: la ampliación y la convención europea: actas de las II jornadas en conmemoración del Día de Europa de la Universidad Pontificia Comillas de Madrid, 8 y 9 de mayo de 2003*, editado por María Susana de Tomás Morales, Christine Heller del Riego, y María Esther Vaquero Lafuente. Madrid: Universidad Pontificia Comillas: 215-228.

COLOMBARA LÓPEZ, Ciro. *Los Delitos de la Ley sobre Abusos de Publicidad*. Santiago de Chile: La Ley, 1996.

COOLEY, Thomas. *Treatise on the Law of Torts*. Chicago: Callaghan & Company, 1888.

CORCUERA ATIENZA, Francisco Javier. "El reconocimiento de los Derechos Fundamentales en la Unión Europea: el final del túnel". En *La protección de los derechos fundamentales en la Unión Europea*, editado por Francisco CORCUERA ATIENZA, 61-98. Madrid: Instituto Internacional de Sociología Jurídica- Dykinson, 2002.

CORRAL TALCIANI, Hernán. "Configuración Jurídica del Derecho a la Privacidad I: origen, desarrollo y fundamentos". *Revista Chilena de Derecho*, nº 27 (2000): 51-79.

CREGO, María Díaz. *Protección de los derechos fundamentales en la Unión Europea y en los estados miembros*. Editorial Reus, Madrid, 2010.

D'ATENA, Antonio. "La Constitución oculta de Europa (antes y después de Lisboa)". *Revista de derecho constitucional europeo*, nº 13 (2010): 17-46.

DAGUERRE GARCÍA, Agustina, ed. "Movimientos migratorios en el mundo: lecturas alternativas y complementarias a los enfoques de seguridad y desarrollo". *Relaciones internacionales: Revista académica cuatrimestral de publicación electrónica,* nº 14 (2010): 5-11.

DARANAS, Manuel. "Sentencia de 15 de diciembre de 1983, Ley del Censo. Derecho a la personalidad y dignidad humana". *Boletín de Jurisprudencia Constitucional (BJC)* (1984): 126-170.

DAVARA FERNÁNDEZ DE MARCO, Isabel. *Hacia la estandarización de la protección de datos personales*. Madrid, España: La Ley, 2011.

DAVOLI, Alessandro. "Fichas técnicas sobre la Unión Europea. La protección de datos personales". Parlamento Europeo, noviembre de 2012. http://www.europarl.europa.eu/ftu/pdf/es/FTU_4.12.8.pdf.

DE FARAMIÑÁN GILBERT, Juan Manuel. "El tratado de Lisboa (un juego de espejos rotos)". *Revista electrónica de estudios internacionales,* nº17 (2009).

DELGADO LIROLA, Isabel. "Terrorismo y cooperación penal: ¿un contexto más favorable para los derechos humanos en las relaciones transatlánticas?". En *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz 2009*. Universidad del País Vasco, (2010): 363-394.

DE HOYOS SANCHO, Montserrat. "Obtención y archivo de identificadores extraídos a partir del ADN de sospechosos: análisis de la regulación española a la luz de la jurisprudencia del Tribunal Europeo de Derechos Humanos". *Revista de Derecho Comunitario Europeo* 14, nº 35 (2010): 93-116.

DE LA FUENTE PASCUAL, Félix. *Glosario jurídico-político de la Unión Europea*. Madrid: Técnos, 2002.

DE LA IGLESIA GARCÍA, Jesús. "La entrada en vigor del Tratado de Lisboa". RUE: *Revista universitaria europea,* nº 12 (2010): 45-60.

DE LUCAS, Javier, y Ernesto VIDAL. "El catálogo de derechos fundamentales en la Constitución española de 1978: ¿una lista cerrada?" En *Introducción a los derechos fundamentales. X Jornadas de Estudio,* vol. 1. Madrid, 1986.

DE MOOR, Alexandra. "The Europol Council Decision: Transforming Europol into an Agency of the European Union". *Common market law review* Vol. 47, Nº 4 (2010): 1089-1121.

DEL MORAL TORRES, Anselmo. "La cooperación policial en la Unión Europea: propuesta de un modelo europeo de inteligencia criminal". *Análisis del Real Instituto Elcano (ARI)* nº 50 (2010): 1-12.

DEL PESO NAVARRO, Emilio. *Ley de protección de datos: la nueva LORTAD*. Ediciones Díaz de Santos, 2000.

DENNINGER, Erhard. "Das Recht auf informationelle Selbstbestimmung und Inere Sicherheit". En *Informationgesellschaft oder Úberwachugstaat del Freiheitsrechte in Computerzitalter*, 291 y ss. Wiesbaden, 1984.

— "El derecho a la autodeterminación informativa". En *Actas de coloquio internacional*. Sevilla: Tecnos, 1987.

DÍAZ DÍAZ, José Enrique. "Cooperación y colaboración internacional en la lucha contra el terrorismo". *Boletín Elcano* nº 90 (2007): 8 y ss.

DÍAZ FERNÁNDEZ, Antonio M. "The evolution of European cooperation in intelligence". *Varia Historia* 28, nº 47 (2012): 163-185.

— "Hacia un nuevo marco Europeo de cooperación en inteligencia". En *Hacia una política europea de inteligencia: ¿reto comunitario o interestatal?*. Barcelona. Instituto de Estudios Internacionales, 2006.

— "La construcción de una capacidad de inteligencia en el seno de la unión europea". En el espacio de libertad, seguridad y justicia de la UE: un balance entre presidencias españolas (2002-2010). *Revista Cidob d'Afers Internacionals*, nº 91, septiembre-octubre 2010.

DÍAZ REVORIO, Francisco Javier, y Eduardo ESPÍN TEMPLADO. "Tribunal Constitucional y creación de derechos 'no escritos'". En *La justicia constitucional en el estado democrático*, de Francisco Javier DÍAZ REVORIO, 231-260. Valencia: Tirant lo Blanch, 2000.

DIETRICH PLAZA, Cristina. "El Tratado de Prüm en el marco de la regulación de la protección de datos personales en la Unión Europea". *Revista de derecho constitucional europeo* nº 7 (2007): 31-64.

— "Las tensiones entre libertad y seguridad en el marco jurídico actual de protección de datos de carácter personal en la Unión Europea". En *Libertad, seguridad y transformaciones del Estado*, editado por Joan Lluís PÉREZ FRANCESCH, 185-213. Barcelona: Institut de Ciències Polítiques i Socials, 2009.

DÍEZ-HOCHLEITNER Rodríguez, Javier, Carmen MARTÍNEZ CAPDEVILA, Irene BLÁZQUEZ NAVARRO, y Javier FRUTOS MIRANDA. "Últimas tendencias en la jurisprudencia del Tribunal de Justicia de la Unión Europea (2008-2011)", La Ley, Madrid, 2012.

EDMOND PETTITI, L. *Enciclopedia Giuridica Treccani*, vol. XXVII, 1991.

EMALDI CIRIÓN, A., E. DOMÍNGUEZ PECO, F. ARANDA GUERRERO, J. LÓPEZ BARJA DE QUIROGA, y J. BAYO DELGADO. *La Protección de Datos en la Cooperación Policial y Judicial*. Pamplona: Aranzadi, 2008.

ESQUINAS VALVERDE, Patricia. *Protección de datos personales en la Policía Europea*. Valencia: Tirant lo Blanch, 2010.

ESTADELLA YUSTE, Olga. *La protección de la intimidad frente a la transmisión internacional de datos personales*. Madrid: Tecnos, 1995.

ETXEBERRÍA GURIDI, José Francisco. "Principio de disponibilidad y protección de datos personales: a la búsqueda del necesario equilibrio en el espacio judicial penal europeo*". Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, nº 23 (2009): 351-366.

FARIÑAS MANTONI, L.M. *El derecho a la intimida*d. Madrid: Trivium, 1983.

FAULL, Jonathan. "Intimidad y seguridad". En *Datospersonales.org: la revista de la Agencia de Protección de datos personales de la comunidad autónoma de Madrid*, nº35 (2008).

FERNÁNDEZ CUESTA, Francisco. "Protección de datos en archivos públicos: introducción a su estudio", Salamanca, (2011). http://gredos.usal.es/jspui/bitstream/10366/111529/3/TG_FernandezCuestaF_Proteccion_datos_archivos.pdf

FERNÁNDEZ GONZÁLEZ, Miguel Ángel. "La defensa de los derechos de las personas y la jurisprudencia del Consejo para la Transparencia". En *Derechos Fundamentales: libro homenaje al profesor Francisco Cumplido Cereceda*. Santiago de Chile: Jurídica de Chile, (2012): 93-108.

FERNANDEZ PASARÍN, Ana. "La dimensión externa del Espacio de Libertad, Seguridad y Justicia: El caso de la cooperación consular local". *Revista CIDOB d'afers internacionals* nº 91 (2010): 87-104.

FERNÁNDEZ TOMÁS, A. "Sobre la eficacia de la Carta de Derechos Fundamentales de la Unión Europea". En *La Carta de Derechos Fundamentales de la Unión Europea*. Zamora: Cuadernos del Instituto Rei Alfonso Henriques de Cooperación Transfronteriza, (2003): 33-48.

FERRI, Giovanni B. "Privacy e libertà informatica". *Banche dati, telemática e diritti della persona* (1984): 45 y ss.

FIGUEROA PLA, Uldaricio. *El sistema internacional y los derechos humanos*. Santiago de Chile: RIL, 2012.

FIODOROVA, Anna. "Cooperación policial internacional en la Unión Europea (II)". http://www.slideshare.net/afiodorova/lisbon-europol-sis-prum-internet.

FLAQUER VILADERBÓ, Lluís Gonzaga. "Tres concepciones de la privacidad". *Sistema: revista de ciencias sociales,* nº 58 (1984): 31-44.

FONTANA, Andrés, Ignacio ROMANO, y Martin VERRIER. "Estrategias de cooperación en materia de seguridad en la Unión Europea" (2012). http://repositorio.ub.edu.ar:8080/xmlui/bitstream/handle/123456789/722/238-fontana.pdf?sequence=1

FONTOURA, Jorge. *O Tratado de Lisboa*, (s. f.).

FRANCHI SCARSELLI, Guido. "Ley Italiana 675 de 1996 sobre privacidad informática". *Revista Derecho del Estado* (2000): 31-43.

FRANCO, Amadeo. "L' informatica guiridica nel diritto costituzionale". *Informatica e ordinamento guiridico* (1992): 27-29.

FREIXES SANJUÁN, Teresa. "La protección de los datos automatizados por el Tribunal Europeo de Derechos Humanos". En *Encuentros sobre Informática y Derecho*, editado por Miguel DAVARA RODRIGUEZ. Pamplona: Aranzadi, 1998.

— "Las principales construcciones jurisprudenciales del Tribunal Europeo de Derechos Humanos". En *Los derechos en Europa*, editado por Yolanda GÓMEZ SÁNCHEZ, 225-244. Madrid: Universidad Nacional de Educación a Distancia, UNED, 1997.

— "Multilevel constitutionalism as general framework for the ascertainment of the legal regulations in the European Union". En *Libertad, seguridad y transformaciones del Estado*, editado por Joan Lluís PÉREZ FRANCESH, 69-80. Barcelona: Institut de Ciències Polítiques i Socials, 2009.

FREIXES SANJUÁN, Teresa, y Juan Carlos REMOTTI CARBONEL. *El futuro de Europa. Constitución y derechos fundamentales.* Valencia: Mimin Ediciones, 2002.

FRÍAS MARTÍNEZ, Emilio. "El acceso a los datos de carácter personal por la Policía. Referencia a los datos de la Seguridad Social". *Noticias Jurídicas*, julio de 2012.

FRIED, Charles. "*Privacy*". *The Yale Law Journal* vol. 77 (1968 de 1967): 475-493.

FROSINI, Tommaso Edoardo. "Nuevas tecnologías y constitucionalismo". *Revista de Estudios Políticos* (Nueva Época) nº 124 (2004): 129-147.

FROSINI, Vittorio. "Banco de datos y tutela de la persona". *Revista de Estudios Políticos* vol. 30 (1982): 21-40.

— *Informática y derecho*. Bogotá: Temis, 1988.

— "La protezione della riservatezza nella societá informática". En *Privacy e banche dei dati*, de N. MATERUCCI, 37 y ss. Bologna, 1981.

GACITÚA ESPÓSITO, Alejandro, *La regulación de la transferencia internacional de datos en España*, Memoria del proyecto final de Master en Auditoria y Protección de Datos, Universidad Autónoma de Barcelona, abril de 2009.

— "La protección de datos de carácter personal en la cooperación policial en materia penal". Trabajo para acreditar la suficiencia investigadora en el Doctorado en Derecho Público, Universidad Autónoma de Barcelona, julio de 2010.

GAMBINO, Silvio. "Jurisdicción y justicia entre Tratado de Lisboa, Convenio Europeo de Derechos Humanos y ordenamientos nacionales". *Revista de derecho constitucional europeo* nº 13 (2010): 83-120.

GARCÍA ANDRADE, Paula. "La geometría variable y la dimensión exterior del espacio de libertad, seguridad y justicia". En *La dimensión exterior del espacio de libertad, seguridad y justicia de la Unión Europea*. Madrid: Iustel, (2012): 87-122

GARCÍA GUTIERREZ, Laura. "TJCE - Sentencia de 18.12.2007, Reino Unido / Consejo, C-77/2005. Creación de la Agencia Frontex - Validez - Exclusión del Reino Unido - Acervo y Protocolo de Schengen". *Revista de Derecho Comunitario Europeo*, Año 13, n° 34 (2009): 1083-1093.

GARCÍA RAMÍREZ, Sergio. *La Jurisprudencia De La Corte Interamericana De Derechos Humanos*. Universidad Nacional Autónoma de México, 2008.

GARCÍA SAN MIGUEL, Luis. *Estudios sobre el derecho a la intimidad*. Madrid: Tecnos, 1992.

GARZÓN CLARIANA, Gregorio. "La protección de los datos personales y la función normativa del Consejo de Europa". *Revista de Instituciones Europeas*, 1981.

— "Los actos delegados en el sistema de fuentes de Derecho de la Unión Europea". *Revista de Derecho Comunitario Europeo* 14, nº 37 (2010): 721-760.

GAY FUENTES, Celeste. *Intimidad y tratamiento de datos en las Administraciones Públicas*. España: Editorial Complutense, 1995.

GONZÁLEZ ALONSO, Luis N. "¿Quién dijo que desaparecen los pilares? La configuración jurídica de la Acción Exterior de la Unión Europea en el Tratado de Lisboa". En *El tratado de Lisboa. La salida de la crisis Constitucional*. Iustel, Madrid (2008): 393 y ss.

GONZÁLEZ CAMACHO, Vicente. "Protección de Datos Personales y cooperación Policial Judicial". Cartagena de Indias, 22 de julio de 2010. http://www.redipd.org/actividades/seminario_2010_cartagena/common/VICEN

TE_GONZALEZ_PD_COOPERACION_POLICIAL_JUDICIAL_CARTAGENA_22_07_2010.pdf.

GONZÁLEZ CAMPOS, Julio, Luis SÁNCHEZ RODRIGUEZ, y María Paz ANDRÉS SÁENZ de SANTA MARÍA. *Curso de Derecho Internacional Público*. 8a ed., 3a en Civitas. Madrid: Thomson-Civitas, 2003.

GONZÁLEZ FUSTER, Gloria. "Privacy and data protection in the EU-security continuum". http://works.bepress.com/serge_gutwirth/71/. Accedido 23 de abril de 2013.

— "Tribunal Europeo de Derechos Humanos: TEDH-Sentencia de 04.12. 2008, S. y Marper c. Reino Unido, 30562/04 y 30566/04-Artículo 8 CEDH-Vida privada-Injerencia en una sociedad democrática-Los límites del tratamiento de datos biométricos de personas no condenadas". *Revista de Derecho Comunitario Europeo*, nº 33 (2009): 619-633.

GONZÁLEZ FUSTER, Gloria. "Protección de datos y cooperación policial y judicial en materia penal en la UE". En *El Proceso Penal en la Sociedad de la Información: Las nuevas tecnologías para investigar probar el delito*, Coordinado por Julio Pérez Gil, La Ley, Madrid, (2012): 587-604.

GONZÁLEZ FUSTER, Gloria, Paul DE HERT, y Serge GUTWIRTH. "Privacy and Data Protection in the EU-Security Continuum ". *International Peace Research Institute (Prio).* junio de 2011.

GONZÁLEZ VALLVÉ, José Luis. "La mayor operación de solidaridad de la historia: crónica de la política regional de la Unión Europea en España" (2006). http://repositori.uji.es/xmlui/handle/10234/34740.

GRENLEAF, Graham. "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108 by Graham Greenleaf: SSRN". *International Data Privacy Law* 2 (19 de octubre de 2011). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960299.

GUASCH PORTAS, Vicente. "Las Transferencias Internacionales de Datos en la Normativa Española y Comunitaria". UNED, 2013. http://e-spacio.uned.es:8080/fedora/get/tesisuned:Derecho-Vguasch/Documento.pdf

GUERRERO PICÓ, María del Carmen. *El Impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*. Thomson Civitas, 2006.

— "Protección de datos personales e Internet: la conservación indiscriminada de los datos de tráfico". *Revista de la Facultad de Derecho de la Universidad de Granada*, n° 8 (2005): 109-139.

GUICHOT REINA, Emilio. "Acceso a la información y protección de datos. Estado de la cuestión". En *Transparencia administrativa y protección de datos personales: V Encuentro entre Agencias Autonómicas de Protección de Datos Personales*, editado por Antonio Troncoso Reigada, Madrid: Thomson-Civitas, (2008): 205-222.

— *Datos personales y administración pública*. Navarra: Thomson-Civitas, 2005.

— *Publicidad y privacidad de la información administrativa*. Editorial Civitas, 2009.

GUTIERREZ ZARZA, María Ángeles. "La protección de datos personales como derecho fundamental del imputado, ¿también en el ámbito del proceso penal?" *La ley penal: revista de derecho penal, procesal y penitenciario* nº 71 (2010): 1 y ss.

GUZMÁN ZAPATER, Mónica. "Cooperación judicial civil y Tratado de Lisboa: entre consolidación e innovación". *Revista General de Derecho Europeo* nº 21 (2010): 2 y ss.

HÄBERLE, Peter. "Derecho constitucional común europeo". En *Derechos humanos y constitucionalismo ante el tercer milenio*. Madrid: Marcial Pons, (1996): 187-224.

HEREDERO HIGUERAS, Manuel. "Estudio crítico de la transposición de la Directiva 95/46/CE en el ordenamiento jurídico español por la L.O. 15/1999 de 13 de diciembre". *Revista Jurídica de Navarra*, nº 31 (2001): 123-140.

– *La Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de carácter Personal: comentario y textos*. Madrid: Tecnos, 1996.

— "La protección de datos personales en manos de la policía: reflexiones sobre el Convenio de Schengen". En *La protecció de dades personals. Regulació nacional i internacional de la seguridad informàtica*. Barcelona: Cetre d' Investigació de la Comunicació i Universidad Pompeu Fabra, (1993): 29-49.

— "La protección de los datos de interés policial y judicial en la Unión Europea: de Shengen a Prüm". *Revista Jurídica de Navarra*, nº 42, (2006): 119-142.

— "La Sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del censo de población". *Documentación administrativa*, nº 198 (1983): 139-159.

HERNÁNDEZ I MORENO, Josep Xabier, María PÉREZ I VELASCO, y Agata SOLERNOU VIÑOLAS. "Reflexiones en torno a la protección de los datos de carácter personal". *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, nº 1 (2005): 21-45.

HERRÁN ORTIZ, Ana Isabel. *El derecho a la intimidad en la nueva Ley orgánica de protección de datos personales*. Madrid: Dykinson, 2002.

— *El derecho a la protección de datos personales en la sociedad de la información*. Bilbao: Universidad de Deusto, 2003.

— "La protección de datos personales en la jurisprudencia constitucional". En *Estudios jurídicos en memoria de José María Lidón*. Universidad de Deusto, (2002): 985-1000.

— *La violación de la intimidad en la protección de datos personales*. Madrid: Dykinson, 1998.

HERRERO DE LA FUENTE, Alberto, ed. *La Carta de Derechos Fundamentales de la Unión Europea: una perspectiva pluridisciplinar*. Valencia: Tirant Lo Blanch, 2003.

HERRERO TEJEDOR, Fernando. *La intimidad como derecho fundamental*. Madrid: Colex, 1998.

HUSTINX, Peter. "Hacia una mayor eficacia de la protección de datos en la Sociedad de la Información". *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid,* nº 50 (2011).

ILLAMOLA DAUSÁ, Mariona. "TJUE - Sentencia de 22.06.2010 (Gran Sala), Aziz Melki y Sélim Abdeli, C-188/10 y C-189/10 - 'Artículo 67 TFUE - Libre circulación de personas - Supresión de controles en las fronteras interiores - Normativa nacional que autoriza controles de identidad a 20 kilómetros de la frontera' - Controles fronterizos y controles de identidad dentro del espacio Schengen." *Revista de Derecho Comunitario Europeo* Año nº 16, Vol. 41 (2012): 205-220.

INDA, F. J. "Schengen: referencia en materia de coordinación policial". Harlax: Ertzainaren lanbide aldizkaria = Revista técnica del Ertzaina n° 11 (1995): 32-93.

INTECO y AEPD. "Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes online". https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Estudios/est_inteco_redesso_022009.pdf.

IRURZUN MONTORO, Fernando. "El diseño institucional de los órganos de cooperación en materia policial y judicial penal: COSI, Europol, Eurojust y el Fiscal Europeo". En *El derecho penal de la Unión Europea: situación actual y perspectivas de futuro*, de Luis Alberto ARROYO ZAPATERO, Adán NIETO MARTÍN, y Marta MUÑOZ DE MORALES ROMERO. Cuenca: Ediciones de la Universidad de Castilla-La Mancha, (2007): 49-68.

JÁUREGUI BERECIARTU, Gurutz, y Juan Ignacio UGARTEMENDÍA ECEIZABARRENA. "Europa en el lecho de Procusto: de la Constitución europea al Tratado de Lisboa". *Revista Vasca de Administración Pública*. Herri-Arduralaritzako Euskal Aldizkaria nº 79 (2007): 105-126.

JUARÉZ PÉREZ, Pilar. "La inevitable extensión de la ciudadanía de la Unión: a propósito de la STJUE de 8 de marzo de 2011 (asunto Ruiz Zambrano)". *Cuadernos de derecho transnacional*, nº 2 (2011): 249-266.

LANZAROT, Ana Isabel Berrocal. "La protección de datos relativos a la salud y la historia clínica en la normativa española y europea". *Revista de la Escuela de Medicina Legal*, nº18 (2011): 12-44.

LASO PÉREZ, José Javier. "Las relaciones exteriores de Europol tras la adopción de la Decisión de 2009 por la que se crea Europol y la entrada en vigor del Tratado de reforma de Lisboa". En *La dimensión exterior del espacio de libertad, seguridad y justicia de la Unión Europea*, de José MARÍN Y PÉREZ DE NANCLARES. Madrid: Iustel, (2012): 314-354.

LÁZPITA GURTUBAN, María. "Análisis comparado de las legislaciones sobre protección de datos de los estados miembros de la Comunidad Europea". Informática y derecho: *Revista iberoamericana de derecho informático*, nº 6-7 (1994): 397-420.

LEZERTÚA RODRÍGUEZ, Manuel. "El espacio jurídico del Consejo de Europa". En *La obra jurídica del Consejo de Europa: (en conmemoración del 60 aniversario del Consejo de Europa)*, Sevilla, Gandulfo, (2010): 27-32.

LIROLA DELGADO, Isabel. "La cooperación judicial en materia penal en el Tratado de Lisboa: ¿un posible proceso de comunitarización y consolidación a costa de posibles frenos y fragmentaciones?". *Revista General de Derecho Europeo*, nº 16 (2008): 3 y ss.

— "Terrorismo y cooperación penal: ¿un contexto más favorable para los derechos humanos en las relaciones transatlánticas?" En *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz 2009*, Universidad del País Vasco, (2010): 363-394.

LOCKE, John. *Segundo Tratado sobre el Gobierno Civil*. Traducido por Carlos Mellizo. Madrid: Alianza, 1994.

LÓPEZ, Antonio. "La investigación policial en Internet: estructuras de cooperación internacional". *IDP: revista de Internet, derecho y política*, nº 5 (2007): 63-74.

LÓPEZ JIMÉNEZ, David. "La protección de datos personales en el ámbito de las redes sociales electrónicas: el valor de la autorregulación". *Anuario de la Facultad de Derecho (Universidad de Alcalá)*, nº 2 (2009): 237-274.

LÓPEZ ROMÁN, Eduardo, y Juan S. MORA. "Un análisis de la estructura institucional de protección de datos en España. Un análisis jurídico y económico de la incidencia de las autoridades de control españolas en la garantía del derecho fundamental de autodeterminación informativa". *Indret - Revista para el análisis del Derecho*, nº 2 (2009): 1-34.

LOYERE, Georges de la. "Flujos transfronterizos y globalización: ¿cómo proteger la intimidad en un mundo global? El papel de las autoridades de protección de datos en materia de transferencias internacionales de datos". *Datospersonales.org/Revista de la Agencia de Protección de Datos de la Comunidad de Madrid* nº 20 (2006): 1 y ss.

LUCAS MURILLO DE LA CUEVA, Pablo. *El derecho a la Autodeterminación Informativa*. Tecnos, 1990.

— *Informática y Protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal).* Madrid: Centro de estudios constitucionales, 1993.

— "La Constitución y el derecho a la autodeterminación informativa". *Cuadernos de Derecho Público*, nº 19-20 (2003): 27-44.

— "La primera jurisprudencia sobre el derecho a la autodeterminación informativa". *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, nº1 (2003).

— "La protección de los datos de carácter personal en el horizonte de 2010". *Anuario de la Facultad de Derecho*, nº 2 (2009): 131-142.

— "Las vicisitudes del derecho de la protección de datos personales". *Revista Vasca de Administración Pública*, nº 58 (2000): 211-242.

— "Perspectivas del derecho a la autodeterminación". *Revista de Internet, Derecho y Política de la UOC*, nº 5 (2007): 18-32.

LUCAS MURILLO DE LA CUEVA, Pablo, y PIÑAR MAÑAS, José Luis. *El derecho a la autodeterminación informativa*. Fundación Coloquio Jurídico Europeo, 2009.

LUENGO ALFONSO, Luis. "Cooperación policial y europol". En *El espacio europeo de libertad, seguridad y justicia, de Ministerio del Interior*, 103-116. Madrid: Ministerio del Interior. Secretaría General Técnica, 2000.

LUQUE GONZÁLEZ, José Manuel. "Schengen. Un espacio de libertad, seguridad y justicia". *Revista de derecho: División de Ciencias Jurídicas de la Universidad del Norte*, n° 21 (2004): 139-149.

MAILLO GONZÁLEZ-ORÚS, Jerónimo. "Diferenciación en el espacio europeo de libertad, seguridad y justicia". En *Unidad y flexibilidad en el futuro de la unión europea: el desafío de las cooperaciones reforzadas*. Madrid: Instituto Universitario de Estudios Europeos de la Universidad CEU San Pablo (2010): 137-163

MANGAS MARTÍN, Araceli. "Evolución del respeto a los derechos humanos en la Unión Europea (teoría y práctica ante los nuevos desafíos del terrorismo)". *Agenda Internacional* nº 26 (2008): 17-36.

MANGAS MARTÍN, Araceli, y Diego LIÑÁN NOGUERAS. *Instituciones y Derecho de la Unión Europea*. 5° ed. Madrid: Tecnos, 2005.

MANGIAMELI, Stelio. *El diseño institucional de la Unión Europea después del Tratado de Lisboa*. Accedido 12 de julio de 2013. http://www.ugr.es/~redce/REDCE15/articulos/10SMangiameli.htm#resumen.

MARICA, Andreea. *El sistema de tratamiento de la información en EUROPOL*. Institut de Ciències Polítiques i Socials WP nº. 309 (2012): 1-33.

— "Génesis de Europol". *Ciencia policial: revista del Instituto de Estudios de Policía* nº 99 (2010): 17-52.

— "INTERPOL y EUROPOL: actores principales en la escena de la seguridad internacional". En *Luces y sombras de la seguridad internacional en los albores del siglo XXI.* Editado por Miguel REQUENA Y DIEZ DE REVENGA, 237-254. Madrid: Instituto Universitario General Gutiérrez Mellado, 2010.

MARTÍN MARTÍNEZ, Magdalena María. "Terrorismo y derechos humanos en la Unión Europea y en el Consejo de Europa: ¿marcos de referencia mundial?" En *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz* 2009, 395-426. Universidad del País Vasco, 2010. http://www.ehu.es/cursosderechointernacionalvitoria/ponencias/pdf/2009/2009_10.pdf.

MARTÍN y PÉREZ DE NANCLARES, José, (coord.). *El Tratado de Lisboa: la salida de la crisis constitucional*. Madrid, Iustel, 2008.

— Ed. *La dimensión exterior del espacio de libertad, seguridad y justicia de la Unión Europea*. Madrid: Iustel, 2012.

— "Seguridad y acción exterior de la unión europea: la creciente relevancia de la dimensión exterior del espacio de libertad, seguridad y justicia". *Revista del Instituto Español de Estudios Estratégicos* 1, nº 1 (2013): 133-152.

MARTÍN y PÉREZ DE NANCLARES, José, y Mariola URREA CORRES. *Tratado de Lisboa*. Madrid: Real Instituto Elcano & Marcial Pons., 2008.

MARTÍNEZ MARTÍNEZ, Ricard. "El derecho fundamental a la protección de datos: perspectivas". *IDP: revista de Internet, derecho y política = revista d'Internet, dret i política* nº 5 (2007): 4 y ss.

— "Los datos de carácter personal en el convenio Europol: las comunicaciones de datos a terceros países". En *XIV Encuentros sobre Informática y Derecho: 2000-2001*, de Miguel Ángel DAVARA RODRIGUEZ, 129-162. Pamplona: Aranzadi, 2001.

— *Tecnologías de la información, policía y constitución*. Valencia: Tirant lo Blanch, 2001.

— *Una aproximación crítica a la autodeterminación informativa*. Madrid: Thomson-Civitas, 2004.

MARTINOTTI, Guido. "La difessa della 'privacy' I". *Politica del diritto* (1971): 749-779.

MARTÍN-RETORTILLO BAQUER, Lorenzo. "El sistema europeo de derechos fundamentales tras la entrada en vigor del Tratado de Lisboa". En *Anuario jurídico de La Rioja* nº15 (2010): 11-98.

MARZO PORTERA, Ana. "Privacidad y cloud computing, hacia dónde camina Europa." *Revista de Ciencias Sociales y Jurídicas* nº 8 (2012): 12-229.

MELLADO PRADO, Pilar. "El funcionamiento de las instituciones en el espacio de libertad, seguridad y justicia". *Revista de derecho de la Unión Europea* nº 10 (2006): 35-49.

MILLÁN MORO, Lucía. "El ordenamiento jurídico comunitario: del Tratado Constitucional al Tratado de Lisboa". *Revista de Derecho Comunitario Europeo 14*, nº 36 (2010): 401-438.

MILLER, Arthur R. "Personal privacy in the Computer Age: the challenge of a new technology and information oriented society". *Michigan Law Review* vol. 67 (1967): 1089-1246.

MIRA ROS, Corazón. "Algunas reflexiones sobre la protección de datos personales en el ámbito judicial". En *actas del IV Congreso Gallego de Derecho Procesal*. Editorial Universidad da Coruña; 581-594. 2012

MONNI, Piero. *L' informaciones: un diritto, un devere, Internaziionale*. Cagliari. (1989)

MONTULL CREMADES, María Ángeles y José Luis PIÑAR MAÑAS. *La Red Iberoamericana de Protección de datos, Declaraciones y Documentos*. Valencia: Tirant Lo Blanch, 2006.

MORENO DOMÍNGUEZ, Juan Francisco. *La carta de los derechos fundamentales de la Unión Europea: desde la solemnidad a la eficacia*. Artículo, 5 de febrero de 2010. http://rabida.uhu.es/dspace/handle/10272/2547.

MORTE GÓMEZ, Carmen, y Guillem CANO PALOMARES. "La interpretación evolutiva y dinámica del Convenio Europeo de Derechos Humanos en la jurisprudencia reciente del Tribunal de Estrasburgo". *Revista general de derecho constitucional* nº 10 (2010): 14 y ss.

MUÑOZ DE MORALES ROMERO, Marta. "Implementation of EU Obligations or Legislative Unseen Offside?: On Fraudulent Shortcuts to Pass (Criminal) Legislation (¿Transposición de Obligaciones Comunitarias o Fuera de Juego Legislativo?: Sobre Los 'Atajos' Fraudulentos Para Adoptar Normas (Penales))". En *Actas del II Congreso de Jóvenes Investigadores en Ciencias Penales*, Salamanca, Forthcoming, 2011.

NINO, Michelle, "The protection of personal data in the fight against terrorism New perspectives of PNR European Union instruments in the light of the Treaty of Lisbon", *Utrecht Law Review* / Volume 6, Issue 1 (January) 2010, pp. 62-85.

NOGUEIRA ALCALÁ, Humberto. *La Constitución reformada de 2005*. Santiago de Chile: Librotecnia, 2005.

NOVOA MONREAL, Eduardo. "*Derecho a la vida privada y libertad de información: Un conflicto de derechos*". México D.F.: Siglo XXI, 1979.

OCDE. *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines* (2011). http://www.oecd-ilibrary.org/science-and-technology/the-evolving-privacy-landscape-30-years-after-the-oecd-privacy-guidelines_5kgf09z90c31-en.

ORAÁ, Jaime, y Felipe GÓMEZ ISA. *La Declaración Universal de los Derechos Humanos: Un Breve comentario en su 50 aniversario*. 2° ed. Bilbao: Universidad de Deusto, 2002.

ORDOÑEZ SOLÍS, David. *Privacidad y protección judicial de los datos personales*. Barcelona: Bosch, 2011.

— "La protección de datos personales en la jurisprudencia europea después del Tratado de Lisboa". En *Últimas tendencias en la jurisprudencia del Tribunal de Justicia de la Unión Europea (2008-2011)*. Madrid: La Ley, 137-170, 2012.

ORTÍ VALLEJO, Antonio. "El nuevo derecho fundamental (y de la personalidad) a la libertad informática (a propósito de la STC 254/1993, de 20 de julio)". En *Derecho privado y Constitución* nº2 (abril de 1994): 305 y ss.

PARDO GETINO, Luis Alfonso. *El principio de respeto de los derechos humanos como fundamento de la construcción europea*. Tesis para optar al grado de doctor. Universidad de León (2009).

PAREJO NAVAJAS, Teresa. "La Carta de los derechos fundamentales de la Unión Europea". *Derechos y Libertades: Revista de filosofía del derecho y derechos humanos* nº 22, (enero de 2010): 205-239.

PAVÓN PÉREZ, Juan Antonio. "La protección de datos personales en el Consejo de Europa: el Protocolo Adicional al Convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales". En *Anuario de la Facultad de Derecho (Universidad de Extremadura) 19-20* (2001-2002): 235-252.

PEGUERA POCH, Miquel. "Derecho y nuevas tecnologías". Barcelona: Editorial UOC, (2005).

PÉREZ CEBADERA, María Ángeles. *Instrumentos de cooperación judicial penal I: la extradición y la euroorden*; publicacions de la Universitat Jaume I, Castellón: (2010).

PÉREZ FRANCESCH, Joan Lluís. "La cooperación policial y judicial en el Tratado de Lisboa, entre la europeización y las reservas estatales". En *Derecho constitucional europeo. Actas del VIII Congreso de la Asociación de Constitucionalistas de España.*, editado por Juan Ignacio UGARTEMENDÍA ECEIZABARRENA y Gurutz JÁUREGUI BERECIARTU, 465-489. Valencia: Tirant lo Blanch, 2011.

— Ed. *Libertad, seguridad y transformaciones del Estado*. Barcelona: Institut e Ciències Polítiques i Socials, 2009.

— "Cooperación policial y judicial en la Convención de Prüm". *Revista de derecho constitucional europeo* nº 7 (2007): 119-136.

— PÉREZ FRANCESCH, Joan Lluís y GIL MÁRQUEZ, Tomás. *El Terrorisme Global*. Ed. UOC, Barcelona, 2009

— "PÉREZ FRANCESCH, Joan Lluís, Tomás GIL, y Alejandro GACITÚA ESPÓSITO. "Informe sobre el PNR. La utilización de datos personales contenidos en el registro de nombres de pasajeros: ¿fines represivos o preventivos?" *Institut de Ciències Polítiques i Socials* 297. Working papers (2011): 1-27.

PÉREZ LUÑO, Antonio Enrique. *Derechos Humanos, Estado de Derecho y Constitución*. Madrid: Tecnos, 2010.

— *Manual de Informática y Derecho*. Barcelona: Ariel, 1996.

— "El derecho a la autodeterminación informativa". En *Anuario de jornadas 1989-1990. (Servicio de Estudios del IVAP)*. Instituto Vasco de Administración Pública, 299-331, (1991).

— "Informática y libertad". *Revista de Estudios Políticos* nº 24 (1981): 31-54.

— "Intimidad y protección de datos personales: del habeas corpus al habeas data". En *Estudios sobre el derecho a la intimidad*, de Luis GARCÍA SAN MIGUEL, 36-45. Madrid: Tecnos, 1992.

— "La contaminación de las libertades en la sociedad informatizada y las funciones del Defensor del Pueblo". *Anuario de Derechos Humanos* nº4. Universidad Complutense de Madrid: (1986-1987): 259-289.

— "Libertad informática y derecho a la autodeterminación informativa". *I Congreso sobre Derecho Informático*, Facultad de Derecho de la Universidad de Zaragoza (1989): 359-375.

— *Nuevas tecnologías, sociedad y derecho. El impacto socio-jurídico de las N. T. de la información*. FUNDESCO. Madrid: (1987)

— "Vittorio FROSINI y los nuevos derechos de la sociedad tecnológica". En *Informatica e diritto, atti della Giornata celebrativa in occasione dei 70 anni di Vittorio Frosini*. Pisa. (1992): 101-112.

PÉREZ LUÑO, Antonio Enrique, Mario LOSANO, y María Fernanda GUERRERO MATEUS. *Libertad informática y Leyes de Protección de Datos*. Centro de estudios constitucionales, 1989.

PÉREZ ROYO, Francisco Javier. *Curso de Derecho Constitucional*. Sexta edición. Madrid: Marcial Pons, 1999.

PFEFFER URQUIAGA, Emilio. *Constitución Política de la República de Chile 2005. Anotada y concordada*. Santiago de Chile: PuntoLEX, 2005.

— *Reformas constitucionales 2005*. Santiago de Chile: Jurídica de Chile, 2005.

PI LLORENS, Montserrat. "El Programa de Estocolmo: el difícil camino hacia la Constitución de una política transversal de derechos humanos en la Unión Europea". En *Hacia una Europa de las personas en el espacio de libertad, seguridad y justicia*, 129-150. Madrid: Marcial Pons, 2010.

— *Los derechos fundamentales en el ordenamiento comunitario*. Barcelona: Ariel, 1999.

PICCA, Georges. "Espacio geográfico y político europeo y cooperación en materia penal". *Eguzkilore: Cuaderno del Instituto Vasco de Criminología* nº 20 (2006): 91-95.

PIÑAR MAÑAS, José Luis. "Protección de datos: origen, situación actual y retos de futuro". En *El derecho a la autodeterminación informativa*, 81-179. Madrid: Fundación Coloquio Jurídico Europeo, 2009.

— "Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio". *Documentos de trabajo (Laboratorio de alternativas)* nº 147 (2009): 1 y ss.

— "Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio". Fundación Alternativas, 2009. Documento de trabajo nº 147.

PIÑAR MAÑAS, José Luis, María José BLANCO ANTÓN, y Álvaro CANALES GIL. *Protección de Datos de Carácter Personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos, La Antigua, Guatemala, 2-6 de junio de 2003)*. Valencia: Tirant Lo Blanch, 2006.

PRIETO ANDRÉS, Antonio. "La nueva directiva europea sobre el tratamiento de datos personales y la protección de la intimidad en el sector de las telecomunicaciones". *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía* nº 5 (2002): 1710-1713.

PRIETO GUTIERREZ, Jesús María. «La Directiva 95/46/CE como criterio unificador», *Revista del Poder Judicial,* n° 48 (1998): 165-243.

PROSSER, William. "*Privacy*". *California Law Review* vol. 48 (1960): 383-423.

PUENTE ESCOBAR, Agustín. "Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal". En *Protección de Datos de Carácter Personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos, La Antigua – Guatemala, 2-6 de julio de 2003),* de José Luis PIÑAR MAÑAS, María José BLANCO ANTÓN, y Álvaro CANALES GIL, 37-67. Valencia: Tirant Lo Blanch, 2006.

QUILEZA AGRADA, Ernesto. "El derecho a la protección de los datos en la jurisprudencia constitucional". Editado por Miguel Ángel DAVARA RODRÍGUEZ. *III Jornadas sobre informática y sociedad* (2001): 187-196.

QUINDIMIL LÓPEZ, Jorge Antonio. "La Unión Europea, FRONTEX y la seguridad en las fronteras marítimas. ¿Hacia un modelo europeo de 'seguridad humanizada' en el mar?". *Revista de Derecho Comunitario Europeo* Año n° 16, n° 41 (2012): 57-118.

RAAB, Charles D., y Collin J. BENNETT. "Protecting Privacy Across Borders: European Policies and Prospects". *Public administration 72*, nº 1 (1994): 95-112.

REBOLLO DELGADO, Lucrecio. *El derecho fundamental a la intimidad*. Madrid: Dykinson, 2000.

— *Vida privada y protección de datos en la Unión Europea*. Madrid: Dykinson, 2008.

REBOLLO DELGADO, Lucrecio, y María Mercedes SERRANO PÉREZ. *Introducción a la protección de datos*. Madrid: Dykinson, 2006.

REMOTTI CARBONELL, José Carlos. "Las medidas contra el terrorismo en el marco del Tratado de Prüm", *Revista de derecho constitucional europeo*, n° 7 (2007): 181–206.

RIBAGORDA GARNACHO, Arturo. "Protección de datos personales. Lecciones aprendidas en el contexto español". Presentado en *XII Jornada Nacional de Seguridad Informática*. Accedido 22 de agosto de 2013. http://www.acis.org.co/fileadmin/Base_de_Conocimiento/XII_JornadaSeguridad/PresentacionArturoRibagorda-Protecciondedatospersonales.pdf.

RÍOS ÁLVAREZ, Lautaro. "Derechos esenciales cuya consagración o amparo están ausentes en nuestra constitución". En *Derechos Fundamentales: libro homenaje al profesor Francisco Cumplido Cereceda*, pp. 357-372. Santiago de Chile: Jurídica de Chile, 2012

— "La reforma de 2005 a la Constitución chilena". *Revista Iberoamericana de Derecho Procesal Constitucional* (2007): 213-231.

RODIER, Claire. "Frontex, el brazo armado de la Europa fortificada". En *El estado del mundo: anuario económico geopolítico mundial* n° 27 (2011): 135-139.

RODOTÀ, Stefano. *Elaboratori elettronici e controllo sociale*. Bolonia: Il Mulino, 1973.

— "Privacy e costruzione della sfera privata. Ipotesi e prospettive". *Politica del diritto* (1991): 525 y ss.

RODRÍGUEZ GARCÍA, Luis Fernando. "Algunas insuficiencias de la normativa europea sobre retención de datos". *Derecho en Sociedad, Revista electrónica de la Facultad de Derecho, ULACIT- Costa Rica* nº3 (julio de 2012): 82 y ss.

RODRÍGUEZ, José Manuel, y Alicia SORROZA BLANCO. "El Espacio de Libertad, Seguridad y Justicia y la próxima Presidencia española de 2010. Parte 1a: la implementación del Tratado de Lisboa y el Programa de Estocolmo". *Análisis del Real Instituto Elcano (ARI)* nº 173 (2009): 1 y ss.

RODRÍGUEZ-IZQUIERDO SERRANO, Miryam. "El terrorismo en la evolución del Espacio de Libertad, Seguridad y Justicia." *Revista de Derecho Comunitario Europeo 14*, nº 36 (2010): 531-559.

RUBIO LLORENTE, Francisco. "Los derechos fundamentales en la Unión Europea y el estatuto de la Carta". *EuropaFutura.org* nº 4 (mayo de 2004): 15-27.

— "Mostrar los derechos sin destruir la Unión". En *La encrucijada constitucional de la Unión Europea: Seminario internacional organizado por el Colegio Libre de Eméritos en la real Academia de Ciencias Morales y Políticas, en Madrid, los días 6, 7 y 8 de noviembre de 2001*, 113-150. Madrid: Civitas, 2002.

RUÍZ CARRILLO, Antonio. *La Protección de Los Datos de Carácter Personal*. Barcelona: Bosch, 2001.

— *Los datos de carácter personal. Concepto, requisitos de circulación, procedimientos y formularios*. Barcelona: Bosch, 1999.

RUIZ JARABO, Pablo. "La Carta de Derechos Fundamentales de la Unión europea y su renuncia a regular la competencia de los tribunales Comunitarios y de Derechos Humanos: ¿Virtud o defecto?". En *Noticias de la Unión Europea* nº 207 (2002): 9-23.

RUÍZ JARABO y COLOMER, Dámaso. "El Tribunal de Justicia de la Unión Europea en el Tratado de Lisboa". En *Noticias de la Unión Europea* nº 291 (2009): 31-40

RUIZ MIGUEL, Carlos. *El Derecho a la Protección de la Vida Privada en la Jurisprudencia del Tribunal Europeo de Derechos Humanos*. Civitas, 1994.

— *La Configuración Constitucional del Derecho a la Intimidad*. Madrid: Tecnos, 1995.

— "El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea". En *La Carta de Derechos Fundamentales de la Unión Europea: una perspectiva pluridisciplinar*, 173-210. Valencia: Fundación Rei Afonso Henriques - Tirant Lo Blanch, 2003.

— "El largo y tortuoso camino hacia la Carta de los Derechos Fundamentales de la Unión Europea". En *Revista europea de derechos fundamentales* nº 2 (2003): 61-90.

— "En torno a la protección de los datos personales". En *Revista de Estudios Políticos* nº 84 (1994): 237-264.

SALDAÑA DÍAZ, María Nieves. "el derecho a la privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego". En *Teoría y Realidad Constitucional* nº 28 (2011): 279-312.

SÁNCHEZ BRAVO, Álvaro. *La protección del derecho a la libertad informática en la Unión Europea*. Sevilla: Universidad de Sevilla, 1998.

SANCHO VILLA, Diana. *Transferencia internacional de datos personales*. Pamplona: Civitas, 2003.

SANTOS VARA, Juan. “El desarrollo de la Oficina Europea de Policía (EUROPOL): el control democrático y judicial”. En *Los Tratados de Roma en su cincuenta aniversario: perspectivas desde la Asociación Española de Profesores de Derecho Internacional y Relaciones Internacionales*, 569-594. Madrid: Marcial Pons, 2008.

SAURA ESTAPA, Jaume. “Comentario al artículo 12 de la Declaración Universal de los Derechos Humanos”. En *La Declaración Universal de los Derechos Humanos*, editado por X PONS RAFOLS, 226-236. Barcelona: Asociación para las Naciones Unidas en España-Icaria, 1998.

SERRANO PÉREZ, María Mercedes. *El derecho fundamental a la protección de datos. Derecho español y comparado*. Madrid: Civitas, 2003.

SERRANO PÉREZ, María Mercedes, y Lucrecio REBOLLO DELGADO. *El derecho fundamental a la intimidad*. 2° ed. Madrid: Dykinson, 2005.

SOLAR CALVO, María del Puerto. “La doble vía europea en protección de datos”. En *Diario La Ley* nº 7832 (2012): 1 y ss.

TÉLLEZ AGUILERA, Abel. *La protección de datos en la Unión Europea*. Madrid: Edisofer, 2002.

— “Nuevas posibilidades de cooperación en la ejecución penal en el marco del Tratado de Lisboa y del Programa de Estocolmo (1)”. En *La ley penal: revista de derecho penal, procesal y penitenciario* nº 74 (2010): 2 y ss.

— *Nuevas Tecnologías. Intimidad y Protección de Datos*. Madrid: Edisofer, 2002.

TIRADO ROBLES, María Carmen. “El refuerzo de la cooperación judicial penal en la Unión Europea: comentario a la Decisión del Consejo 2009/426/JAI, de 16 de diciembre de 2008”. En *Revista General de Derecho Europeo* nº 21 (2010).

TONIATTI, Roberto. “Libertad informática y derecho a la protección de datos personales: principios de legislación comparada, en II Jornada de Estudio sobre la «protección de datos y derechos fundamentales”. *Anuario de Jornadas (1989-1990)* (1991): 255-352.

TORRES, José Luis. “Uso de las nuevas tecnologías en la gestión integral de fronteras realizado por FRONTEX para combatir la criminalidad organizada transnacional”. En *La seguridad y la defensa en el actual marco socio-económico: nuevas estrategias frente a nuevas amenazas*, editado por Miguel REQUENA y DÍEZ DE REVENGA, 217-244. Madrid: Instituto Universitario General Gutiérrez Mellado, 2011.

TRONCOSO REIGADA, Antonio. “La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional”. *Cuadernos de Derecho Público* nº 19-20 (2003): 231-334.

— *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*. 1a ed. Madrid: Civitas, 2010.

— "El derecho al olvido en Internet a la luz de la propuesta de Reglamento General de Protección de Datos Personales". En *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid* nº 59 (2012).

— El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibro en los modelos de protección de datos a nivel internacional". En *Revista Internacional de Protección de Datos Personales* nº1 (julio-diciembre de 2012): 4-41.

— *La protección de datos personales: en busca del equilibrio*. Valencia: Tirant lo Blanch, 2010.

— "Hacia un nuevo marco jurídico europeo de la protección de datos personales". *Revista española de derecho europeo* nº 43 Civitas. (2012): 25-184.

URIARTE, Mikel. "El tratamiento de datos personales en la determinación del riesgo". En *Chile y la Protección de Datos Personales. ¿Están en Crisis Nuestros Derechos Fundamentales*?, de Raúl ARRIETA CORTÉS, 37-46. Santiago de Chile: Universidad Diego Portales, 2009.

URREA CORRES, Mario. "El control de fronteras exteriores como instrumento para la seguridad: una aproximación al nuevo marco jurídico de frontex". En *Revista del Instituto Español de Estudios Estratégicos* nº 0 (2012): 153-172.

— "El control de fronteras de la Unión Europea y su dimensión exterior: algunos interrogantes sobre la actuación de FRONTEX". En *La dimensión exterior del espacio de libertad, seguridad y justicia de la Unión Europea*, 235-254. Madrid: Iustel, 2012.

VACAREZZA Y., Ricardo, y Elena NÚÑEZ M. "¿A quién pertenece la Ficha Clínica?" *Revista médica de Chile 131*, nº 1 (2003): 111-114.

VILASAU SOLANA, Mónica. "La Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. privacidad." En *IDP: revista de Internet, derecho y política, revista d'Internet, dret i política* nº 3 (2006): 1-15.

VILLAVERDE MENÉNDEZ, Ignacio. "La jurisprudencia del Tribunal Constitucional sobre el derecho fundamental a la protección de datos de carácter personal". En *La protección de datos de carácter personal en los centros de trabajo*, de Antoni FARROLÍS I SOLÁ, 48-63. Madrid: Cinca: Fundación Francisco Largo Caballero, 2006.

— "Protección de datos personales, derecho a ser informado, y autodeterminación informativa del individuo. A propósito de la STC 254/1993". En *Revista Española de Derecho Constitucional* nº 41 (agosto de 1994): 187 y ss.

WALTER, Jean-Philippe. "Perspectivas para la intimidad y la seguridad". En *Datospersonales. org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid* nº 34 (2008): 3 y ss.

WARREN, Samuel D., y Louis D. BRANDEIS. "The Right to Privacy". *Harvard Law Review vol. IV*, nº 5 (15 de diciembre de 1890).

WARREN, Samuel D., y Louis D. BRANDEIS. "El derecho a la intimidad". Traducido por Benigno PENDAS y Pilar BASELGA. Madrid: Civitas, 1995.

WASSENBERG, Birte. *History of the Council of Europe* (2013),

WESTIN, Alan. *Privacy and Freedom*. New York: Atheneum, 1970.

ZAFFARONI, Eugenio Raúl. "La legitimación del control penal de los "extraños"." *Dogmática y criminología*. *Dos visiones complementarias del fenómeno delito* (2004): 625-650. Disponible en http://cuadernos.inadi.gob.ar/cuadernos-del-inadi-01.pdf

ZAMBRANO GÓMEZ, Esperanza. "La regulación de los ficheros policiales en España y su tratamiento en la Convención de Prüm: la perspectiva de las autoridades nacionales de protección de datos". En *Revista de derecho constitucional europeo* nº 7 (2007): 167-180.

— "La regulación de los ficheros policiales en España y su tratamiento en la Convención de Prüm: la perspectiva de las autoridades nacionales de protección de datos". *Revista de derecho constitucional europeo* nº 7 (2007): 167-180.

ZAMORA CRESPO, Mara. "Visados, asilo, inmigración y otras políticas relacionadas con la libre circulación de personas". En *Políticas comunitarias: bases jurídicas*, editado por Antonio Calonge Velázquez, 113-138. Valladolid: Lex Nova, 2002.

ZAPATER DUQUE, Esther. "La dimensión exterior del espacio de libertad, seguridad y justicia en el Programa de Estocolmo: el reto de la integración y de la coherencia". En *¿Hacia una Europa de las personas en el espacio de libertad, seguridad y justicia?*, 19-44. Madrid: Marcial Pons, 2010.

ZILLER, Jacques. "El tratado de Prüm". En *Revista de derecho constitucional europeo* nº 7 (2007): 21-30.