TESIS para optar al grado de Doctora en Derecho.

Programa: Las Administraciones Públicas
en el estado social y democrático de Derecho.
Análisis Jurídico Administrativo.
Departamento Responsable: Derecho Público.

UNIVERSIDAD DE MÁLAGA

IMPLICACIONES INSTITUCIONALES DE LA LEY DE PROTECCIÓN DE DATOS

Doctoranda: Mª Belén Sánchez González.

Directores: Dr. Ángel Sánchez Blanco y

Dr. Juan Antonio Robles Garzón.

Málaga, Noviembre 2015

A mi esposo, Guillermo.

" Internet…es un don de Dios.

No tengan miedo de hacerse ciudadanos del mundo digital".

Papa Francisco

Mensaje para la XLVIII Jornada Mundial de las Comunicaciones Sociales.

"Comunicación al Servicio de una Auténtica Cultura del Encuentro"

Índice.

Agradecimientos.

Esta tesis ha sido fruto de muchas horas y del amor de muchas personas.

GRACIAS en primer lugar a mis padres. A mi madre María que me acompaña cada día, y a mi padre José que también lo hace desde el cielo. Ellos han sido mis pilares, mi vida y mi razón de ser, el espejo en el que mirarme cada día para intentar ser mejor persona. Me lo han dado todo, y sin ellos este trabajo no habría llegado nunca. Gracias papá porque sé que tú eres el artífice de esta aventura.

GRACIAS a mi marido, Guillermo, mi gran amor, a quien admiro profundamente por sus principios y con quien comparto el valor del trabajo, del esfuerzo y el amor a nuestra familia.

GRACIAS a mis niñas, Belén y Ester, por ser el tesoro más preciado de mi vida. Por su belleza interior, por el ánimo, por la ayuda y por la comprensión mostrada a pesar del tiempo robado.

GRACIAS a mis hermanos Pablo, Rafa, Francis y Jero, por ser los eslabones inseparables de mí misma, por estar siempre ahí, por ser uno.

GRACIAS al Dr. Ángel Sánchez Blanco, por ser el causante. Su profesionalidad unida a sus cualidades personales lo hacen merecedor de mi más profundo reconocimiento.

GRACIAS al Dr. Juan Antonio Robles, ese magnífico profesor que confió en mí y me ha mantenido unida al mundo académico durante mi vida profesional.

GRACIAS a Leonardo Cervera por prestarme su ayuda incondicional en este proyecto y abrirme las puertas de Europa.

Abreviaturas.

AC	Autoridad de Control
ACC	Autoridad Común de Control
AEPD	Agencia Española de Protección de Datos.
AN	Audiencia Nacional
ANC	Autoridades Nacionales Competentes.
APD	Autoridades de Protección de Datos.
APDCAT	Agencia Catalana de Protección de Datos.
APEC	Foro de Cooperación Económica Asia – Pacífico.
API	*Advance Passenger Information.*
ARCO	Acceso, Rectificación, Cancelación y Oposición
BCE	Banco Central Europeo.
BCR	Binding Corporate Rules
BOCG	Boletín Oficial de las Cortes Generales
BOE	Boletín Oficial del Estado.
C	Caso
CAHDATA	*Comité ad hoc data*
CBPR	*Cross Border Privacy Rules*
CdE	Consejo de Europa
CDFUE	Carta de Derechos Fundamentales de la Unión Europea.
CDR	Comité de las Regiones
CE	Constitución Española de 1978.
CE	Comunidad Europea

CECA	Comunidad Europea del Carbón y del Acero
CEDH	Convenio Europeo de Derechos Humanos.
CEE	Comunidad Económica Europea
CEEA	Comunidad Europea de Energía Atómica
CEPD	Consejo Europeo de Protección de Datos
CESE	Comité Económico y Social
CETS	*Council of Europe Treaty Series*
CIL	*Correspondant Informatique et Libertés.*
CM	Consejo de Ministros
COM	Comunicación
CORA	Comisión para la Reforma de las Administraciones Públicas
CPO	*Chief Privacy Officer o Corporate Privacy Officer.*
CRID	*Centre de Recherches Informatique et Droit.*
CSIG	*Cloud Select Industry Group.*
DO	Diario Oficial
DOCE	Diario Oficial de las Comunidades Europeas.
DOUE	Diario Oficial de la Unión Europea
DPO	*Data Protection Officer.*
DSC	Diario de Sesiones del Congreso
DUDH	Declaración Universal de Derechos Humanos.
EDPS	*European Data Protection Supervisory*
EEE	Espacio Económico Europeo
EEUU	Estados Unidos
ETS	*European Treaty Series*
EU	*Europe Union*

EURODAC	Base de datos dactiloscópicos informatizada de la Unión Europea.
EUROJUST	Unidad de Cooperación Judicial Europea.
EUROPOL	Oficina Europea de Cooperación Policial.
FRA	*Fundamental Rights Agency.*
FRONTEX	Agencia Europea para la gestión de la cooperación operativa en las fronteras exteriores de los Estados miembros de la Unión.
FTC	*Federal Trade Commission*
GT29	Grupo de Trabajo del artículo 29
ICO	*Information Commissioner´s Office*
IITF	*Information Infrastructure Task Force.*
IMI	Sistema de Información del Mercado Interior
IoT	*Internet of Things*
IWGDPT	*International Working Group on Data Protection in Telecommunications*
JAI	Consejo de Justicia y Asuntos de Interior o Cooperación policial y judicial en materia penal
LGT	Ley General de Telecomunicaciones.
LIBE	Comisión de Libertades Civiles, Justicia y Asuntos de interior de la Unión Europea.
LOPD	Ley Orgánica de Protección de Datos de Carácter Personal
LORTAD	Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.
LSSI	Ley de Servicios de la Sociedad de la Información
MLAA	*Mutual Legal Assistance Agreement*
MoU	*Memorandum of Understanding*
MUS	Mecanismo Único de Supervisión.
OCDE	Organización para la Cooperación y el Desarrollo Económico.
OECE	Organización Europea de Cooperación Económica

OMB	*Office of Management and Budget.*
ONG	Organización no Gubernamental
ONU	Organización de las Naciones Unidas.
OPERA	Oficina para la Ejecución de la Reforma de la Administración
PIA	*Privacy Impact Assesment*
PNR	*Passenger Name Records.*
RDLOPD	Reglamento de desarrollo de la Ley Orgánica de Protección de Datos Personales.
REC	Recomendación
RGPD	Reglamento General de Protección de Datos
SEPD	Supervisor Europeo de Protección de Datos.
SH	*Safe Harbour*
SIA	Sistema de Información Aduanera.
SIS	Sistema de Información Schengen.
SIS II	Sistema de Información Schengen de segunda generación
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
STJCE	Sentencia del Tribunal de Justicia de las Comunidades Europeas
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
TC	Tribunal Constitucional.
TEDH	Tribunal Europeo de Derechos Humanos.
TFUE	Tratado de Funcionamiento de la Unión Europea.
TIC	Tecnologías de la información y la comunicación.
TJCE	Tribunal de Justicia de las Comunidades Europeas.
TJUE	Tribunal de Justicia de la Unión Europea
TTIP	*Trasatlantic Trade and Investment Partnership*
TUE	Tratado de la Unión Europea

UE	Unión Europea
UK	*United Kingdom*
VIS	*Visa Information System*
VVAA	Varios
WCO	*World Customs Organisation*
WPISP	*Working Party on Information Security and Privacy*

1 Introducción.

1.1 Presentación.

Desde que finalicé mi licenciatura, la relación del Derecho y las nuevas tecnologías han sido una constante en mi desarrollo profesional. Soy de esa generación que comenzó trabajando con un 342 y una impresora matricial, y hoy vive enganchada al *smartphone*, eso sí, de última generación, un miniordenador que me permite hacer casi de todo. Las implicaciones jurídicas en el progreso tecnológico me han entusiasmado siempre, y el asesoramiento jurídico en nuevas tecnologías lo incorporé desde un principio a los servicios que prestaba a los clientes. Pero entender este mundo no es fácil viniendo del Derecho. Acudí a profesionales de la ingeniería y la informática para adquirir nociones básicas que me permitieran comprender unas leyes en las que los conceptos que se manejaban eran absolutamente técnicos.

Y me apasionaba la protección de datos. Aún no sé bien por qué, quizás por mis profundas convicciones del derecho a la privacidad, por el respeto a las personas o simplemente por esa conexión tan interesante entre el Derecho y la tecnología. Los de Derecho no somos sólo gente de letras. Para escribir las letras hay que entender el mundo, y el mundo sobre el que escribes te tiene que gustar. Esta es mi mayor aportación hacia mí misma con este trabajo: he disfrutado y aprendido muchísimo.

Vengo de una familia donde los valores del esfuerzo y la excelencia se inculcan desde pequeños, y la Universidad es un agente fundamental en el progreso académico y personal. Hice mis cursos de tesis hace unos años, y el paso del tiempo y la vida me hicieron dejar este proyecto de lado, aunque siempre albergando el deseo de desarrollarlo. Mi relación con el mundo universitario y la Facultad de Derecho ha permanecido constante a lo largo de mis años gracias a Juan Antonio Robles. Pero la fortuna de cruzarme con Ángel Sánchez Blanco reavivó mi sueño convirtiéndolo en una realidad. La decisión de llevar adelante una tesis requería, en mi caso, del apoyo de mi familia, pues la logística diaria de una madre, hija, esposa y

profesional no es compatible con cerrar las puertas de tu casa y ponerte a investigar. Mi familia, como siempre, mi gran apoyo. Todos a una. Bendita familia.

Como no podía ser de otra manera, mi investigación tenía una temática clara, la protección de datos; y un objetivo también claro desde los inicios, las Autoridades de control.

1.2 Planteamiento del problema.

Los que formamos parte de esta profesión sabemos que el derecho va siempre detrás de la realidad, pero en el caso de las nuevas tecnologías elaborar una ley *ad hoc* para cada tecnología que aparece en escena supone su obsolescencia más absoluta antes de llegar siquiera al debate parlamentario.

¿A quién miramos todos los días los que trabajamos en la protección de datos? A la Agencia Española de Protección de Datos. La razón, la inmediatez. La Ley Orgánica de Protección de Datos ha variado muy poco desde 1999, por lo que la conocemos sobradamente. Pero las problemáticas que se planteaban desde su aprobación hicieron que la AEPD multiplicara exponencialmente el trabajo que inicialmente tenía. La aplicación de la LOPD necesitaba de interpretaciones constantes, y la Agencia supo hacerlo y muy bien. Hemos utilizado sus criterios, informes y resoluciones a diario, no sólo en la fase de incumplimientos y procedimientos sancionadores, sino sobre todo en la fase preventiva, aplicando sus criterios en la implementación de políticas de protección de datos a los distintos agentes de la sociedad. Así pues, la Agencia se ha convertido en el interlocutor inmediato de los profesionales, y esa cualidad la ofrece fundamentalmente a través de la divulgación de su trabajo, y muy especialmente en su página web. Por ello, para mí, la Agencia ha sido siempre un referente.

La mayoría de las personas tiene la sensación de que las brechas de seguridad que pueden ocurrir en el tratamiento de sus datos vienen del mundo internet. Pero esto no es del todo cierto. Internet es un conducto más y existen muchas normas y control a

nivel internacional que intentan proteger a las personas. La gran incógnita está en cómo garantizar los derechos de los ciudadanos en los nuevos paradigmas del desarrollo tecnológico, sobre los que además existe el determinismo más absoluto en las generaciones de jóvenes actuales y en las que están por llegar. ¿Cómo se protegen los datos personales en el *cloud computing*, en las aplicaciones de los *smartphones* o en la información captada por los drones? ¿Y la que transmitimos a través del *wearable*, la geolocalización o las aplicaciones de sanidad móvil? ¿Qué pueden hacer con nuestros datos? ¿Qué consecuencias tendrá para las personas el uso del *big data*?.

El derecho fundamental a la protección de datos vive una segunda etapa. Hemos conseguido su reconocimiento a todos los niveles, dotándolo de un haz de derechos y disposiciones del ciudadano difícilmente comparable con otros derechos. Pero el inexorable devenir de la tecnología hace que la protección del derecho se desplace hacia el tratamiento más que a la propia captación de los datos en sí misma.

La violación del derecho a la protección de datos de carácter personal produce efectos inmediatos de incalculable dimensión. La instancia judicial es totalmente insuficiente. Por ello se hacen necesarias instituciones que ayuden a los ciudadanos y a las empresas a actuar con diligencia, que difundan la cultura de la protección de datos, que supervisen la aplicación de la ley y que sean capaces de hacer cumplir la misma. Estas instituciones son las Autoridades de control de Protección de Datos.

1.3 Objeto de la investigación.

Tal y como he expuesto anteriormente, en mis horas frente al ordenador trabajando para solventar problemas en relación con el tratamiento de datos han sido muchos los recursos que he utilizado de la Agencia Española de Protección de Datos, pero muchos también de la Agencia de Protección de Datos de Madrid, una Agencia que ha contribuido en gran medida a la difusión y cultura de la materia. Como andaluza que soy, y haciendo patria, siempre quise que mi Andalucía tuviera un organismo similar que contribuyera al conocimiento y difusión del derecho y que a la vez

desarrollara competencialmente un área que contribuiría a su reconocimiento y desarrollo autonómico.

Ese fue mi objetivo inicial, el análisis de la Autoridad de control autonómica y su engranaje en el sistema nacional y europeo. En ese ínterin se aprobó la Ley de Transparencia Andaluza que creaba el órgano. El análisis inicial de este organismo me hizo tomar conciencia del alcance de mi estudio.

Cualquier aproximación a una institución requiere del conocimiento a fondo de las competencias y la materia de la misma.

Comencé analizando el derecho fundamental en España a la protección de datos, y todos los documentos, bibliografía y jurisprudencia que estudiaba me remitían a Europa, sobre todo al Convenio 108 del Consejo de Europa. Allá donde leas protección de datos aparecerá el Convenio 108. Así que decidí cambiar la sistemática de mi estudio y comencé a trabajar el derecho a la protección de datos en Europa. Ha sido un gran trabajo que me ha reportado mucho conocimiento. No es lo mismo defender el derecho fundamental a la protección de datos porque sí, porque lo es, que defenderlo conociendo su construcción, su configuración y sus límites. El objeto de mi estudio se amplió desproporcionadamente. Quería conocer a fondo cómo funcionan todas las Autoridades de control en protección de datos, pero el alcance era mucho mayor del que había pensado, así que tuve que ponerle límites.

Decidí focalizar el estudio en el Supervisor Europeo de Protección de Datos, la Agencia Española de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía, analizando sus orígenes, características y sus funciones, su necesidad y su conveniencia.

1.4 Metodología.

El enfoque metodológico ha sido múltiple: mi propia experiencia profesional, bibliografía, jurisprudencia, recursos de internet, reuniones y estancias en los organismos.

Partía de la base de mi conocimiento profesional de la materia.

Como buena investigadora decidí buscar toda la bibliografía específica acerca del tema, pero no todos los temas tenían bibliografía suficiente, pues parte del análisis ha sido sobre temas absolutamente novedosos.

La Jurisprudencia fue, evidentemente, base indiscutible sobre la que analizar la creación y consagración del derecho a la protección de datos, la ponderación con otros derechos, los problemas de competencias entre organismos, la interpretación de las normas, las características de las autoridades de control y la legitimidad de estas. La jurisprudencia examinada ha sido fundamentalmente del Tribunal Constitucional, del Tribunal de Justicia de la Unión Europea y del Tribunal Europeo de Derechos Humanos.

Pero si desde un principio hay una herramienta que he empleado a diario esa ha sido internet, la gran biblioteca del mundo. He utilizado muchos recursos de internet, sobre todo páginas de organismos oficiales. Esta tesis se ha cerrado el siete de noviembre de 2015, y he incluido datos publicados el día seis.

Fundamental en mi investigación ha sido la estancia en Bruselas en la oficina del Supervisor Europeo de Protección de Datos, en los que mi visión europeísta, que ya existía, se afianzó hasta convertirme en una férrea defensora de Europa. Tuve la suerte de ver in situ cómo trabajan las distintas áreas del Supervisor, mantuve reuniones con los Jefes de Unidad y vi como la transparencia de la organización y la preparación de los recursos humanos son el gran activo de la institución. También mantuve reuniones en el Parlamento Europeo y en la Comisión con quienes trabajan en la Unidad de Protección de Datos; unos, redactores del nuevo Reglamento General de Protección de Datos; y otros, verdaderas instituciones que trabajan día a día en la elaboración del texto definitivo que será la normativa a aplicar en toda Europa, cuyas conversaciones me enseñaron más que todo lo que pudiera estudiar durante meses desde mi mesa de trabajo.

Quise extrapolar la experiencia con la Agencia Española de Protección de Datos y también tuve la suerte de compartir una jornada más que provechosa con quienes

están al frente en el área internacional, el área que se llevará gran parte del trabajo con las modificaciones de aplicación del nuevo Reglamento General de Protección de Datos.

A nivel de Comunidad Autónoma he hecho un seguimiento constante a las novedades regulatorias y a la comunicación de la Junta de Andalucía, si bien el organismo aún no está constituido y no es posible analizar su funcionamiento.

He asistido a jornadas y foros sobre protección de datos, seguridad, autoridades de control y novedades regulatorias en Europa, y también me he entrevistado con delegados de protección de datos de multinacionales.

Las dificultades metodológicas en la investigación han venido de la propia temática a la que aludíamos al principio: las nuevas tecnología, el cambio, la inmediatez…

Desde mi análisis, han sido cuatro los principales factores que han dificultado en cierta manera el estudio: 1.- la escasez de bibliografía sobre parte de la temática; 2.- la bibliografía en materia europea estaba publicada fundamentalmente en inglés, y alguna en francés; 3.- el análisis pormenorizado de los tres textos a debate en el nuevo Reglamento General de Protección de Datos (la propuesta de la Comisión, las enmiendas presentadas por el Parlamento Europeo y el texto aportado por el Consejo) además de la propuesta realizada por el propio Supervisor Europeo de Protección de Datos, (fuera evidentemente del proceso legislativo ordinario) para colaborar con su visión a las negociaciones del trílogo (las negociaciones a tres bandas entre Comisión, Parlamento y Consejo); y 4.- los cambios normativos habidos en los últimos tiempos.

Este último aspecto lo desgloso con algo más de detenimiento. En los últimos meses antes de cerrar este trabajo se han generado tres situaciones directamente determinantes para el trabajo de campo. Me refiero en primer lugar al Reglamento General de Protección de Datos (téngase en cuenta que la versión de la Comisión es de junio de 2012 y la del Parlamento de marzo de 2014), habiéndose presentado el texto del Consejo en junio de 2015, la propuesta del Supervisor es de julio, y a partir de ahí opiniones e informes varios del Supervisor, Grupo de Trabajo del Artículo 29,

Autoridades de control nacionales, etc. En segundo lugar la sentencia del Tribunal de Justicia de la Unión Europea de seis de octubre de 2015, caso *Schrems* vs Comisión, en la que el Tribunal ha declarado inválida la Decisión de la Comisión de 26 de julio de 2000 (2000/520/CE) por la que se establecía un Acuerdo con EEUU (Acuerdo de Puerto Seguro –*Safe Harbour*-) que garantizaba la transferencia de datos personales desde la UE a EEUU. Esta sentencia ha generado la inmediata intervención de los organismos internacionales y las Autoridades de control de todos los países de la Unión, además de un estado de opinión generalizado a nivel mundial. A fecha de cierre de esta investigación se está negociando un nuevo acuerdo con EEUU que según comunicó la Comisión el seis de noviembre deberá cerrarse en tres meses. Y en tercer lugar la publicación en el BOE el dos de octubre de los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía.

1.5 Contenido de la investigación.

La tesis se divide en tres grandes capítulos, cuyo criterio de división ha sido el territorio: Europa, Estados Unidos y España. En todos ellos se estudia el origen del derecho a la protección de datos, los instrumentos normativos, la jurisprudencia (en su caso) y los organismos encargados de su supervisión o tutela, sobre los que se focaliza el desarrollo de la investigación. A lo largo del trabajo existen referencias constantes a las Autoridades de control, pues en todo momento se han intentado poner en relación (argumentando su necesidad o su aportación) con los distintos enfoques y áreas analizadas.

El primer capítulo es el tratado con mayor profundidad y que contiene las principales aportaciones de esta investigación, dadas las novedades que supone una nueva normativa de protección de datos directamente aplicable a todos los países de la Unión Europea. Se han distinguido tres grandes secciones: el Consejo de Europa, las Directrices Internacionales y la Unión Europea. El Consejo de Europa como origen de los Derechos Humanos junto con el Convenio 108 conforman la base jurídica de toda la normativa posterior europea e internacional del derecho a la protección de

datos de carácter personal. Las Directrices de la OCDE y de la ONU marcan también los orígenes de la protección de datos, hasta llegar a nuestros días donde los Estándares Internacionales de la Resolución de Madrid del año 2009 suponen el reconocimiento internacional a un derecho que todos los estados miembros quieren garantizar a sus ciudadanos, y todo ello de la mano de Autoridades de control independientes. Para completar la visión internacional analizamos también el Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico (APEC). Por su parte, el estudio de la Unión Europea se llevará la parte más importante de nuestro trabajo, desde la creación del derecho fundamental hasta la normativa europea, examinando la Directiva 95/46/CE de Protección de Datos, el Reglamento (CE) 45/2001 que regula el tratamiento de datos personales en las instituciones de la Unión Europea, la Carta de los Derechos Fundamentales y el nuevo Reglamento General de Protección de Datos. Finaliza este bloque con un análisis pormenorizado de las Autoridades Europeas de Protección de Datos, haciendo especial énfasis en el Supervisor Europeo de Protección de Datos y en el nuevo Consejo Europeo de Protección de Datos, que sustituye al Grupo de Trabajo del Artículo 29, valorando la nueva situación que se creará en Europa con este Reglamento y esta nueva Institución. Profundizamos sobre las características de los organismos de control y en especial sobre la independencia.

En el segundo capítulo intentamos hacer un paralelismo entre los modelos estadounidense y europeo, buscando las similitudes y diferencias, para lo que explicamos el concepto de privacidad y la protección que EEUU le otorga, así como el tratamiento dado por el principal organismo que tutela los derechos de los ciudadanos en materia de privacidad, la Comisión Federal del Comercio (*Federal Trade Commission.)*. Sometemos a análisis el Asunto *Safe Harbour* por cuanto la repercusión a nivel europeo ha cobrado dimensiones extraordinarias y es el caso más mediático actualmente entre los agentes económicos.

El tercer capítulo lo dedicamos a España, donde se analiza el reconocimiento del derecho fundamental a la protección de datos como derecho atípico y el reparto competencial existente teniendo en cuenta que ni la materia ni la competencia son reconocidas en la Constitución española. Examinamos la normativa al respecto y

desglosamos con especial interés la naturaleza, estructura y funcionamiento de la Agencia Española de Protección de Datos, en la que describimos todas las nuevas competencias que el nuevo Reglamento General de Protección de Datos otorga a las Autoridades de control nacionales. A nivel autonómico estudiamos las Autoridades de control autonómicas, como son Cataluña, País Vasco y Andalucía, con referencias a la extinta Agencia de Madrid, intentando valorar la problemática de las competencias asumidas por cada una de ellas. Hacemos un análisis más pormenorizado del Consejo Andaluz de Protección de Datos que si bien aún no ha comenzado su andadura, ya tiene naturaleza propia *ex lege*.

2 CAPÍTULO I. Legislación y Supervisión en Europa.

2.1 Antecedentes. El Consejo de Europa.

2.1.1 El Convenio Europeo de Derechos Humanos.[1]

La historia del mundo, y la de Europa por ende, se incardina en una sucesión de luchas y guerras sobre las que sus ciudadanos se han sobrepuesto y mejorado[2]. Nuestra Europa, cuna de cultura, tráfico de gentes y progreso siempre ha dado un paso adelante tras acontecimientos que han devastado a sus pueblos. De cada crisis los europeos han creado una oportunidad de mejora. Es así como se unen al proyecto de Naciones Unidas que vio la luz definitivamente el 24 de octubre de 1945 con la firma de la Carta de las Naciones Unidas.

Bajo el paraguas de la ONU fue donde por vez primera se estableció en un instrumento jurídico internacional un derecho a la protección de la esfera privada de las personas frente a la intrusión de otros, especialmente del Estado; y lo hizo en la Declaración Universal de Derechos Humanos de las Naciones Unidas, en 1.948, donde *"La Asamblea General proclama la DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS como ideal común por el que todos los pueblos y naciones deben esforzarse, a fin de que tanto los individuos como las instituciones, inspirándose constantemente en ella, promuevan, mediante la enseñanza y la educación, el respeto a estos derechos y libertades, y aseguren, por medidas progresivas de carácter nacional e internacional, su reconocimiento y aplicación*

[1] Consejo de Europa, Convenio Europeo de Derechos Humanos, CETS Nº 5, Roma 1950.
[2] Es interesante hacer mención aquí al nuevo proyecto sobre el que trabaja la Unión Europea, La Casa de la Historia Europea, institución cultural para el debate sobre la historia europea que tendrá su sede en Bruselas y prevé su apertura para 2016.

universales y efectivos, tanto entre los pueblos de los Estados Miembros como entre los de los territorios colocados bajo su jurisdicción"[3].

Tras la II Guerra Mundial, y en paralelo al proceso anterior, Europa sintió la necesidad y la obligación de defender los derechos humanos y el Estado de Derecho donde habitara el imperio de la ley, y ello desde la cooperación entre sus países, para lo que creó la primera organización internacional en el continente. Así nació El Consejo de Europa, con el Tratado de Londres el 5 de mayo de 1949[4], naciendo un organismo interestatal europeo constituido a fecha de hoy por 47 países de Europa, a excepción de Bielorrusia (por no reunir las características de país democrático) y Ciudad de Vaticano, que está como país observador[5].

En el objetivo del Consejo de Europa de conseguir un área democrática a lo largo de todo el continente europeo en el que el respeto a los Derechos Fundamentales y al Estado de Derecho fuera la misma premisa, se firmó en Roma el Convenio Europeo de Derechos Humanos (CEDH) el 4 de noviembre de 1950 que entró en vigor en 1953, teniendo todos los Estados miembros dicho convenio incorporado a su legislación nacional.

Para garantizar el cumplimiento de estos derechos, el Consejo de Europa creó en 1959 el Tribunal Europeo de Derechos Humanos (TEDH), el cual admite la

[3] Declaración Universal de Derechos Humanos (DUDH) de las Naciones Unidas (ONU). Asamblea General, resolución 217 A (III), de 10.12.1948, artículo 12: *"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".*

[4] Tratado de Londres. CETS nº1, 1949.
Artículo 1: *"a) La finalidad del Consejo de Europa consiste en realizar una unión más estrecha entre sus miembros para salvaguardar y promover los ideales y los principios que constituyen su patrimonio común y favorecer su progreso económico y social. b) Esta finalidad se perseguirá, a través de los órganos del Consejo, mediante el examen de los asuntos de interés común, la conclusión de acuerdos y la adopción de una acción conjunta en los campos económicos, social, cultural, científico, jurídico y administrativo, así como la salvaguardia y la mayor efectividad de los derechos humanos y las libertades fundamentales. c) La participación de los Miembros en los trabajos del Consejo de Europa no debe alterar su contribución a la obra de las Naciones Unidas y de las restantes organizaciones o uniones internacionales de las: que formen parte. d) Los asuntos relativos a la defensa nacional no son de la competencia del Consejo de Europa".*

[5] Los 28 estados de la Unión Europea son miembros del Consejo de Europa.

legitimación activa de personas físicas, grupos de personas físicas, ONG, o personas jurídicas ante la denuncia de violaciones del Convenio[6].

El derecho a la protección de datos personales forma parte de los derechos que se protegen en el CEDH[7], y a lo largo de su historia, el TEDH ha examinado en numerosas ocasiones denuncias planteadas en materia de protección de datos, tales como la interceptación de las comunicaciones telefónicas[8] o las injerencias en la vida privada por acceso a datos médicos.[9]

2.1.2 El Convenio 108 y su Protocolo Adicional.[10]

La evolución de las nuevas tecnologías y el flujo interfronterizo de datos hizo que el Consejo de Europa detectara la necesidad de una regulación específica del derecho a la protección de datos de carácter personal dentro del derecho a la vida privada. En la década de los setenta, el Comité de Ministros tuvo que adoptar numerosas resoluciones en este ámbito, en relación a la protección otorgada por el artículo 8 del CEDH.[11]

[6] Sobre el Convenio Europeo de Derechos Humanos, ver WHITE, R. AND OVEY, C., *The European Convention on Human Rights*, Oxford, Oxford University Press, 2010.

[7] Convenio Europeo de Derechos Humanos (CEDH). 1950. Artículo 8.1: *"Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia".*

[8] Véase, por ejemplo, STEDH núm. 8691/79, de 2 de agosto de 1984, Malone contra el Reino Unido: *"La medición global de las comunicaciones telefónicas (origen, destino, duración), cuando se efectúan para un fin distinto de su objetivo único de contabilidad, aunque en ausencia de cualquier intervención, como tal, constituye una injerencia en la vida privada".*

[9] Por ejemplo, STEDH, I. contra Finlandia, nº 20511/03, de 17 de julio de 2008: *"Lo que se requiere… es una protección real y efectiva que excluya cualquier posibilidad de acceso no autorizado como la ocurrida. No se dio esta protección. El Tribunal no puede sino concluir que… el Estado no cumplió con su obligación, de conformidad con el artículo 8.1 del Convenio… de garantizar respeto por la vida privada de la demandante".*

[10] Ver TÉLLEZ AGUILERA, A. *La protección de datos en la Unión Europea. Divergencias normativas y anhelos unificadores*, Edisofer, Madrid, 2002, p.26-58; también ARENAS RAMIRO, M. La Protección de datos personales en los países de la Unión Europea, Revista Jurídica de Castilla y León núm. 16, 2008, p. 113- 163.

[11] Consejo de Europa, Comité de Ministros, Resolución (73) 22 relativa a la protección de la vida privada de las personas físicas en relación con los bancos de datos electrónicos en el sector privado, de 26 de septiembre de 1973; Consejo de Europa, Comité de Ministros (1974), 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, de 20 de septiembre de 1974.

"Teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados… Reafirmando al mismo tiempo su compromiso en favor de la libertad de información sin tener en cuenta las fronteras… Reconociendo la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos…", el Consejo de Europa adopta en 1981 el Convenio 108 que regula la protección de datos de carácter personal.[12]

Su objetivo era y es garantizar el respeto al derecho fundamental a la protección de datos, el cual se asienta en siete principios: consentimiento, información, control, calidad, lealtad, seguridad y confidencialidad.[13] Serán estos principios los que posteriormente den cuerpo a todas las normativas de protección de datos en el continente. Por vez primera se desarrolla un glosario de términos y se aplica a todos los sectores públicos y privados, permitiendo excepciones a su aplicación en situaciones como la seguridad del Estado. Se comienza también a hablar de la posibilidad de ampliar el ámbito de aplicación a datos no automatizados -cuestión importante que refleja una visión de futuro-; establece el principio de calidad de los datos, así como las especiales medidas de seguridad para los datos sensibles. Enumera los derechos del titular de los datos al acceso y rectificación a los mismos, y solicita a los estados miembros que reconozcan un sistema de sanciones y recursos en el derecho interno que permita la efectividad del derecho. También crea un nuevo órgano: un Comité Consultivo que mediante propuestas mejore la aplicación o presente propuestas de enmiendas, con miras a facilitar o mejorar la aplicación del Convenio, al tiempo que toma parte en la labor normativa, redactando documentos que son generalmente aplicables[14].

Es interesante resaltar cómo ya en este Convenio se acuerda que cada Estado miembro nombrará una autoridad (o varias) competente para informar a los otros

[12] Consejo de Europa, Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. CETS nº 108, Estrasburgo 1981.

[13] Sobre la protección de datos en la Unión Europea, ver CAREY, P. *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press, 2009; DELGADO, L. *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L., 2008; DESGENS-PASANAU, G., *La protection des données à caractère personnel*, París, LexisNexis, 2012.

[14] Convenio 108. CETS nº 108. Capítulo V.

estados acerca del derecho interno en materia de protección de datos en el ámbito de la colaboración para el flujo transfronterizo de datos[15]. Esta es la antesala del Protocolo Adicional al Convenio 108 del año 2001[16], sobre el establecimiento obligatorio de Autoridades nacionales de control, las cuales son investidas por mandato de este Protocolo de la mejor de las cualidades para un organismo de control o consultivo, que posteriormente será característica fundamental de todas las que quedarán por venir, la independencia[17].

España ratificó el Convenio 108 el 31 de enero de 1984, pero no fue hasta la promulgación de la LORTAD (Ley 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal), cuando nuestro país cumplió con sus obligaciones jurídico-internacionales establecidas en el texto normativo, referidas precisamente a la elaboración de la mencionada legislación interna y explicitadas en el artículo 4 del Convenio[18].

El esfuerzo jurídico por parte de El Consejo de Europa para desarrollar el contenido del Convenio nº 108 se ha ido desplegando a través de distintas Recomendaciones sectoriales dirigidas a los gobiernos de los estados miembros sobre temas

[15] Convenio 108. CETS nº 108. Capítulo IV.

[16] Consejo de Europa, Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencia de datos, en lo que respecta a las autoridades de control y los flujos transfronterizos de datos, CETS nº 181, 2001.

[17] Protocolo Adicional Convenio 108. CETS nº 181, 2001. Artículo 1.3.

[18] Artículo 4 Convenio 108: *"1. Cada Parte tomará, en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos enunciados en el presente capítulo.*
2. Dichas medidas deberán adoptarse a más tardar en el momento de la entrada en vigor del presente Convenio con respecto a dicha Parte".
En este sentido RIPOLL CARULLA, S. "En torno a la calificación de la pasividad española en el cumplimiento del Convenio nº 108 de Europa como acto ilícito internacional", en *La Responsabilidad Internacional*, XIII Jornadas de la AEPDIRI, Alicante 1990, p. 313-330.
También PAVÓN PÉREZ, J.A. en *"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 de la Universidad de Extremadura nº 19-20. 2001-2002, p. 235 a 252.
El 25 de noviembre de 1986, el portavoz del Grupo Parlamentario Mixto Juan María Bandrés Molet, formuló una Proposición no de Ley en la que *"insta al Gobierno español para que sin demora cumpla las obligaciones derivadas del Convenio 108 del Consejo de Europa, relativo a la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, mediante el inmediato desarrollo de nuestro derecho interno, de forma que los derechos de los ciudadanos puedan ser ejercidos de manera compatible con el contenido de aquel Convenio Internacional".* Boletín Oficial de las Cortes núm. 20, de 4 de diciembre de 1986. La Comisión Constitucional, en sesión del 11 de marzo de 1987, desestimó dicha proposición.

específicos. Así nos encontramos con Recomendaciones en el ámbito laboral[19], acerca de pagos[20], sobre cuestiones de datos médicos[21], seguridad social[22], datos relativos a la actividad policial[23], a la administración[24], al seguro[25], al márketing[26], a temas estadísticos[27] o a internet[28].

El Protocolo Adicional de 2001 tiene como objetivo la creación de Autoridades de control en los países miembros que sean responsables del cumplimiento de los principios establecidos en el Convenio así como del flujo transfronterizo de datos[29], dotándoles de poderes de investigación y de intervención, pudiendo iniciar procedimientos legales o judiciales en caso de que se produzca la violación del derecho interno y conocer de las reclamaciones que realicen los ciudadanos relativas

[19] Consejo de Europa. Recomendación CM/ Rec (2015) 5 del Comité de Ministros sobre el tratamiento de datos personales en el contexto laboral, aprobada el 1 de abril de 2015; que sustituye la Recomendación nº R (89) 2, sobre la protección de datos de carácter personal utilizados con fines de empleo de 18 de enero de 1989.

[20] Consejo de Europa. Recomendación nº R (90) 19 sobre la protección de los datos personales utilizados para el pago y otras operaciones relacionadas. 13 de septiembre de 1990.

[21] Consejo de Europa. Recomendación nº R (97) 5 sobre la protección de datos médicos, aprobada el 13 de febrero de 1997, que sustituye a la Recomendación nº R (81) 1 sobre las regulaciones para los bancos de datos médicos automatizados de 23 de enero de 1981.

[22] Consejo de Europa. Recomendación nº R (86) 1 sobre la protección de datos de carácter personal utilizados con fines de seguridad social. 23 de enero de 1986.

[23] Consejo de Europa. Recomendación nº (87) 15 que regula el uso de los datos personales en el sector de la policía. 17 de septiembre de 1987.

[24] Consejo de Europa. Recomendación nº R (91) 10 sobre la comunicación a terceros de los datos personales en poder de los organismos públicos. 9 de septiembre de 1991.

[25] Consejo de Europa. Recomendación nº R (2002) 9 sobre la protección de los datos personales recogidos y tratados a efectos del seguro. 18 de septiembre de 2002.

[26] Consejo de Europa. Recomendación nº R (85) 20 sobre la protección de los datos personales utilizados para fines de venta directa. 25 de octubre de 1985.

[27] Consejo de Europa. Recomendación nº R(97) 18 relativa a la protección de los datos personales recogidos y tratados con fines estadísticos, aprobada el 30 de septiembre de 1997; y que sustituye a la Recomendación nº R(83)10 sobre la protección de datos de carácter personal utilizada para la investigación y la estadística científica, de 23 de septiembre de 1983.

[28] Consejo de Europa. Recomendación CM / Rec (2012) 3 del Comité de Ministros en materia de protección de derechos humanos con respecto a los motores de búsqueda, de 4 de abril de 2012;
Recomendación CM / Rec (2012) 4 del Comité de Ministros en materia de protección de derechos humanos con respecto a las redes sociales, de 4 de abril de 2012;
Recomendación CM/Rec (2010) 13 del Comité de Ministros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles, de 23 de noviembre de 2010;
Recomendación Nº R (99) 5 sobre la protección de la privacidad en Internet, de 23 de febrero de 1999;
Recomendación nº R (95) 4, sobre la protección de datos de carácter personal en el ámbito de los servicios de telecomunicaciones, con especial referencia a los servicios telefónicos, de 7 de febrero de 1995.

[29] Protocolo Adicional del Convenio 108. CETS nº 181, 2001. Artículo 1.1.

a derechos y libertades fundamentales en el tratamiento de los datos personales[30]. Este poder de investigación descrito en la Memoria Explicativa del Protocolo, consiste en la posibilidad de solicitar información relativa al tratamiento de los datos personales y de obtenerlo, haciéndolo accesible en particular, cuando una persona ejerce sus derechos previstos en la normativa nacional, y ello en virtud del artículo 8 del Convenio. El poder de la intervención, siguiendo con la Memoria Explicativa del Protocolo, puede adoptar diversas formas en el derecho interno, siendo ejemplo de ello cuando la autoridad obliga al responsable del fichero a rectificar, borrar o destruir datos inexactos o recolectados ilícitamente; cuando emite medidas cautelares o dictámenes previos a la ejecución de las operaciones de tratamiento de datos; o cuando remite casos a los Parlamentos nacionales u otras instituciones del Estado. El tercer punto fundamental que trata este artículo primero del Protocolo Adicional es la independencia de las Autoridades de control[31]. Destaca la Memoria Explicativa como elementos que contribuyen a salvaguardar dicha independencia la composición del órgano, el método de designación de sus miembros, la duración del ejercicio, las condiciones del cese de sus funciones, la asignación de recursos suficientes o la adopción de decisiones sin estar sujeto a órdenes o mandatos externos. Por último se reconoce en este instrumento la posibilidad de que las decisiones de estas Autoridades puedan ser recurridas judicialmente[32] y les insta a que exista una cooperación adecuada entre ellas[33].

El Convenio 108 del Consejo de Europa es, a fecha de hoy, el único instrumento jurídico a nivel internacional vinculante en materia de protección de datos, ya que está abierto a la firma de países no miembros del Consejo de Europa, lo que hace que su alcance sea universal. Son parte contratantes 45 estados de Europa (siendo San Marino el último en acceder, en marzo de 2015) y Uruguay. Actualmente Marruecos, Mauritania y Senegal han sido invitados por el Comité de Ministros a adherirse[34]. También cabe la posibilidad de solicitar ser observador en el Comité, tal y como han hecho por ejemplo Canadá o Australia.

[30] Protocolo Adicional del Convenio 108. CETS nº 181, 2001. Artículo 1.2.
[31] Protocolo Adicional del Convenio 108. CETS nº 181, 2001. Artículo 1.3.
[32] Protocolo Adicional del Convenio 108. CETS nº 181, 2001. Artículo 1.4.
[33] Protocolo Adicional del Convenio 108. CETS nº 181, 2001. Artículo 1.5.
[34] Disponible en: http://www.coe.int/t/dghl/standardsetting/DataProtection/default_en.asp.

El 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 fue adoptado el 23 de mayo de 2001 por el Comité de Ministros del Consejo de Europa y abierto para la firma el 8 de noviembre de 2001, en Estrasburgo, exigiéndose para su entrada en vigor la ratificación del mismo por 5 estados firmantes del Convenio, lo cual ocurrió el 1 de julio de 2004. Actualmente ha sido ratificado por 36 estados[35]. El Comité Consultivo del Convenio fue el encargado de elaborar el proyecto de protocolo en su decimoquinta reunión celebrada del 16 al 18 de junio de 1999, y de llevarlo al Comité de Ministros para su remisión a la Asamblea Parlamentaria.

La adhesión al Convenio 108 por parte de estados que no forman parte del Consejo de Europa supone que puedan convertirse en miembros de pleno derecho del Comité y beneficiarse así del foro que supone dicho órgano para intercambiar conocimientos e información. Además, el país que se adhiere obtiene una garantía para que pueda tener lugar la transferencia recíproca de datos personales, cuestión ésta de extrema importancia y a valorar por países como los EEUU al haberse invalidado recientemente la Decisión de la Comisión[36] (Acuerdo de Puerto Seguro) que permitía a las empresas estadounidenses adheridas al Acuerdo realizar la transferencia internacional de datos de carácter personal con Europa. Dicho de otro modo, el asunto *Schrems* contra Facebook[37] ha dejado en una situación muy delicada a las empresas europeas que transfieren datos a Estados Unidos. Sería un buen momento para plantearse por parte de éstos últimos su incorporación a dicho instrumento. El caso tiene sus orígenes en la demanda colectiva de 25 ciudadanos europeos –asunto

[35] La lista de los estados parte del Convenio 108 y del Protocolo de 2001 pueden consultarse en la siguiente dirección: http://conventions.coe.int/Treaty/Commun/Cherchesig.asp?NT=108&cl=eng.

[36] Decisión 2000/520/CE de la Comisión de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.
DOCE L 215; por la cual se establecen las condiciones que han de cumplir las entidades estadounidenses para adherirse a dicho Acuerdo.
La lista de entidades estadounidenses adheridas a los principios de Puerto Seguro está disponible en http://www.export.gov/safeharbor.

[37] STJUE de 06.10.2015. Asunto C-362/14, *Schrems* vs Comisión.

PRISM- contra Facebook[38], encabezada por el joven *Schrems*, en el cual, el Alto Tribunal de Irlanda elevó una cuestión de prejudicialidad ante el TJUE a efectos de su pronunciamiento sobre si la Autoridad de control de Protección de Datos está vinculada por la Decisión de la Comisión[39] a pesar de los artículos 7, 8 y 47 de la Carta de Derechos Fundamentales de la Unión Europea y el artículo 25.6 de la Directiva 95/46/CE, y por lo tanto no podía entrar a valorarla; o bien podía realizar su propia investigación del asunto a la luz de la evolución de los hechos que se habían ido desarrollando desde que se publicó dicha Decisión. En definitiva, si el Acuerdo de Puerto Seguro[40] entre los EEUU y Europa podía ser analizado por la Autoridad de Control. El Tribunal de Justicia ha decidido que el acuerdo es nulo, y por lo tanto las entidades que hasta el momento se acogían a dicho acuerdo no pueden ahora garantizar como venían haciendo hasta el momento, que su flujo de datos fuera de la Unión Europea tiene un nivel de protección adecuado. El 23 de septiembre de 2015 se hicieron públicas las conclusiones del Abogado General *Yves Bot* en dicho asunto[41], según las cuales la decisión de la Comisión por la que se declaraba el carácter adecuado de la protección de los datos personales en Estados Unidos no impedía que las autoridades nacionales suspendieran la transferencia de datos de los usuarios europeos de Facebook a servidores situados en Estados Unidos, llegando a considerar incluso nula tal decisión por cuanto no contenía garantías suficientes, argumentación que hizo suya el Tribunal, dictando sentencia en sentido

[38] Este asunto ha dado lugar al movimiento "*Europe vs Facebook*". Disponible en: http://www.europe-v-facebook.org/prism/facebook.pdf.

[39] Decisión 2000/520/CE de la Comisión de 26 de julio de 2000, conocido como "Acuerdo de Puerto Seguro".

[40] Ver 36.

[41] Comunicado de prensa 106/15, del Tribunal de Justicia de la Unión Europea. Luxemburgo 3 de septiembre de 2015. Disponible en: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-09/cp150106es.pdf.
Considera *Bot* en sus alegaciones que la existencia de una decisión de la Comisión que declara que un país tercero garantiza un nivel de protección adecuado de los datos personales transferidos no puede anular, ni tan siquiera reducir, las facultades que tienen las autoridades nacionales de control en virtud de la Directiva sobre el tratamiento de datos personales, pues la facultad de intervención de las Autoridades de Control nacionales debe permanecer íntegra. Para el Abogado General la independencia de la que deben gozar estas Autoridades estaría limitada si estuvieran vinculadas en términos absolutos por las decisiones de la Comisión. Bot entiende además que la Decisión 2000/520[41] sobre adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada es nula, y ello porque de las de las apreciaciones llevadas a cabo tanto por la *High Court of Ireland* como por la propia Comisión se desprende que la normativa y la práctica de Estados Unidos permiten recopilar a gran escala los datos personales de los ciudadanos de la UE que se transfieren, sin que éstos tengan derecho a una tutela judicial efectiva, demostrando así que la Decisión de la Comisión no contiene garantías suficientes.

favorable a las conclusiones de *Bot*[42]. Finalmente, el TJUE declaró inválida la Decisión, si bien profundizaremos en este asunto en el Capítulo 2.

Por todo ello consideramos que sería una buena solución en la protección del tratamiento de datos de carácter personal realizada con los Estados Unidos que este país se adhiriera al Convenio núm. 108 del Consejo de Europa. En la era de la globalización y de la utilización de Internet, el Convenio 108 y su Protocolo Adicional tienen una ventaja esencial: su dimensión transfronteriza. Estos instrumentos contienen garantías para proteger el movimiento transfronterizo de datos hacia terceros países, asegurando en principio a los estados firmantes un nivel de protección adecuado.

En el año 2010, el Comité Consultivo del Convenio 108 inició un proceso de revisión del citado instrumento, en el cual tras dos años de trabajo, 2011 y 2012, elaboró un

[42] Sentencia TJUE de 6 de octubre de 2015. Asunto C-362/14, entre *Maximillian Schrems* y *Data Protection Commissioner.*
"La petición de decisión prejudicial tiene por objeto la interpretación de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»), de los artículos 25, apartado 6, y 28 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 (DO L 281, p. 31), en su versión modificada por el Reglamento (CE) nº 1882/2003 del Parlamento Europeo y del Consejo, de 29 de septiembre de 2003 (DO L 284, p. 1) (en lo sucesivo, «Directiva 95/46»), así como, en sustancia, la validez de la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (DO L 215, p. 7)".
Concluye la sentencia: *"En virtud de todo lo expuesto, el Tribunal de Justicia (Gran Sala) declara: 1) El artículo 25, apartado 6, de la 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 su versión modificada por el Reglamento (CE) nº 882/2003 del Parlamento Europeo y del Consejo, de 29 de septiembre de 2003, entendido a la luz de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que una Decisión adoptada en virtud de la referida disposición, como la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46, 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, por la que la Comisión Europea constata que un tercer país garantiza un nivel de protección adecuado, no impide que una autoridad de control de un Estado miembro, a la que se refiere el artículo 28 de esa Directiva, en su versión modificada, examine la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona alega que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado.*
2) La Decisión 2000/520 es inválida".

documento técnico de reforma que remitió al Consejo de Ministros del Consejo de Europa. Este documento está siendo estudiado por un Comité *ad hoc* (CAHDATA)[43] y pese a tener una hoja de ruta inicial más corta en el tiempo, la última actualización del mismo es de abril de 2015[44].

Recientemente, María *Michaelidou, programme advisor* de la Unidad de Protección de Datos del Consejo de Europa, ha puesto de manifiesto los esfuerzos del Consejo de Europa en el proceso de actualización del Convenio 108[45], siendo los objetivos fundamentales reforzar la protección al abordar nuevos retos y fortalecer los mecanismos de seguimiento, pretendiendo que se promueva como un estándar universal, siendo una herramienta con un carácter sencillo, flexible y pragmático, que garantice la coherencia y compatibilidad con otros marcos normativos, en especial el nuevo Reglamento General de Protección de Datos[46].

Tal y como expuso *Michaelidou* en el VII Foro de la Privacidad[47], las principales novedades de la propuesta del texto actualizado recaen fundamentalmente en el ámbito de aplicación, principios básicos, datos sensibles, obligaciones del responsable del tratamiento, seguridad, flujo transfronterizo de datos, Autoridades de control y el Comité Consultivo.

Si comparamos el borrador del Convenio 108 y el borrador del Reglamento General de Protección de datos (aunque tenga varias versiones - la de la Comisión, la del

[43] *Ad hoc Committee on Data Protection*. Comité creado por el Comité Consultivo del Convenio 108.

[44] Para ver el último borrador, de abril de 2015:
http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/CAHDATA%203_Report_CM(2015)40_En.pdf.
Para consultar la trayectoria y la agenda de trabajo:
http://www.coe.int/t/dghl/standardsetting/dataprotection/Cahdata_en.asp. .

[45] MICHAELIDOU, M. VII Foro de la Privacidad. Ponencia: *"Council of Europe data protection standards and the modernization of Convention 108".* Data Privacy Institute, ISMS Forum. Madrid 22.09.2015.

[46] Considerando 81 bis del nuevo Reglamento General de Protección de Datos, propuesta del Consejo de la Unión Europea, de 11 de junio de 2015: *"Aparte de los compromisos internacionales adquiridos por el tercer país u organización internacional, la Comisión también deberá tener en cuenta las obligaciones derivadas de la participación del tercer país u organización internacional en sistemas multilaterales o regionales, en particular en relación con la protección de datos personales, así como la ejecución de dichas obligaciones. En particular, debería tenerse en cuenta la adhesión del país al Convenio adoptado el 28 de enero de 1981 por el Consejo de Europa relativo a la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo adicional…"*

[47] Ver 45.

Parlamento y la del Consejo-), podemos observar una alineación casi total entre ambos textos.

Al analizar dichas novedades profundizando en el último borrador del Convenio 108 al que venimos haciendo referencia, vemos que efectivamente en cuanto al ámbito de aplicación, no distingue datos automatizados o no, sino que se aplica a todo tipo de tratamiento y excluye del mismo los tratamientos en el ámbito doméstico[48]. En materia de principios básicos, los que se ven más desarrollados en relación al texto anterior afectan a la legitimación, la proporcionalidad y la exactitud de los datos[49]. Asimismo, los datos sensibles son descritos con mayor precisión, y detalla cuáles son[50]. Por su parte, se amplían las obligaciones del responsable del tratamiento, ya que se obliga a implementar medidas de seguridad, facilitar al titular de los datos información acerca del responsable del tratamiento, de la finalidad del mismo, de las categorías de datos, de los destinatarios de los datos si los hubiere o los medios para

[48] Art. 3. 1. del borrador del Convenio 108 actualizado, version abril 2015 (ver 44): *" Each Party undertakes to apply this Convention to data processing subject to its jurisdiction in the public and private sectors, thereby securing every individual's right to protection of his or her personal data.*
1bis. This Convention shall not apply to data processing carried out by an individual in the course of [purely] personal or household activities".

[49] Artículo 5 del borrador del Convenio 108 actualizado, versión abril 2015 (ver 44).
"Legitimacy of data processing and quality of data.
1. Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake.
2. Each Party shall provide that data processing can be carried out on the basis of the free, specific, informed and unambiguous4 consent of the data subject or of some other legitimate basis laid down by law.
3. Personal data undergoing processing shall be processed lawfully.
4. Personal data undergoing processing shall be:
a. processed fairly and in a transparent manner;
b. collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for historical, statistical and scientific purposes is, subject to appropriate safeguards, compatible with those purposes;
c. adequate, relevant and not excessive in relation to the purposes for which they are processed; d. accurate and, where necessary, kept up to date;
e. preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed."

[50] Artículo 6 del borrador del Convenio 108 actualizado, versión abril 2015 (ver. 44):
"Special categories of data. 1. The processing of: - genetic data; - personal data relating to offences, criminal proceedings and convictions, and related security measures; - biometric data uniquely identifying a person; - personal data for the information they reveal relating to racial origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life; shall only be allowed where specific and additional appropriate safeguards are enshrined in law, complementing those of this Convention".

ejercer sus derechos[51]. La seguridad también se aborda con mayor precisión que en el texto anterior, ya que además de obligar a la implementación de medidas de seguridad tanto para el responsable como para el encargado del tratamiento a fin de evitar accesos no autorizados, destrucción, pérdida, uso, modificación o revelación de datos, la novedad más relevante es la obligación de notificar a las Autoridades de control las brechas de seguridad que puedan afectar al derecho fundamental[52]. El flujo transfronterizo de datos adquiere un desarrollo importante en el nuevo texto, permitiendo el flujo de datos entre países miembros del Convenio o, en caso de no serlo, cuando el tercer país u organización tenga un nivel adecuado de protección, el cual se acreditará mediante la ley existente en ese estado –incluidos los acuerdos y convenios internacionales de los que sea parte- o acuerdos específicos realizados por instrumentos vinculantes y ejecutables de los que las Autoridades de control de cada país tendrán toda la información así como de aquellas transferencias que se realicen al amparo de determinadas excepciones[53].

---

[51] Artículo 7 bis del borrador del Convenio 108, versión abril 2015 (ver 44):
*"Transparency of processing**.** 1. Each Party shall provide that the controller informs the data subjects of: a. the controller's identity and habitual residence or establishment; b. the legal basis and the purposes of the intended processing; c. the categories of personal data processed; d. the recipients or categories of recipients of the personal data, if any; and e. the means of exercising the rights set out in Article 8".*

[52] Artículo 7 del borrador del Convenio 108 actualizado, versión abril 2015 (ver 44):
"Data security.
1. Each Party shall provide that the controller, and, where applicable the processor, takes appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data.
2. Each Party shall provide that the controller shall notify, without delay, at least the competent supervisory authority within the meaning of Article 12bis of this Convention, of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects".

[53] Artículo 12 del borrador del Convenio 108 actualizado, versión abril 2015 (ver 44):
Transborder flows of personal data.
"1. A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention. Such a Party may however do so if bound by harmonised rules of protection shared by States belonging to a regional international organisation.
2. When the recipient is subject to the jurisdiction of a State or international organisation which is not Party to this Convention, the transfer of personal data may only take place where an appropriate level of protection based on the provisions of this Convention is secured.
3. An appropriate level of protection can be secured by:
a. the law of that State or international organisation, including the applicable international treaties or agreements; or
b. ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing.

Las Autoridades de supervisión, cuya creación en el ámbito del Convenio 108 se hizo a través del Protocolo Adicional de 2001, tienen un lugar importante en el nuevo texto de modernización del Convenio 108[54]. Se obliga a la existencia de una Autoridad de control, o supervisora, que tendrán las siguientes facultades:

4. Notwithstanding the provisions of the previous paragraphs, each Party may provide that the transfer of personal data may take place if:

a. the data subject has given explicit, specific and free consent, after being informed of risks arising in the absence of appropriate safeguards; or

b. the specific interests of the data subject require it in the particular case; or

c. prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society.

5. Each Party shall provide that the competent supervisory authority within the meaning of Article 12bis of this Convention is provided with all relevant information concerning the transfers of data referred to in paragraph 3.b and, upon request, paragraphs 4.b and 4.c.

6. Each Party shall also provide that the supervisory authority is entitled to request that the person who transfers data demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests and that the supervisory authority may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject to condition such transfers.

7. Exceptions to the provisions of this Article are allowed insofar as they constitute a necessary and proportionate measure in a democratic society for the freedom of expression".

[54] Artículo 12 bis del borrador del Convenio 108, versión abril 2015 (ver 44).

"Supervisory authorities.

1 Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the provisions of this Convention.

2 To this end, such authorities:

a. shall have powers of investigation and intervention;

b. shall perform the functions relating to transfers of data provided for under Article 12, notably the approval of standardised safeguards;

c. shall have powers to issue decisions with respect to violations of the provisions of this Convention and may, in particular, impose administrative sanctions;

d. shall have the power to engage in legal proceedings or to bring to the attention of the competent judicial authorities violations of the provisions of this Convention;

e. shall promote:

i. public awareness of their functions and powers as well as their activities;

ii. public awareness of the rights of data subjects and the exercise of such rights;

iii. awareness of controllers and processors of their responsibilities under this Convention;

specific attention shall be given to the data protection rights of children and other vulnerable individuals.

2bis. The competent supervisory authorities shall be consulted on proposals for any legislative or administrative measures which provide for the processing of personal data.

3. Each competent supervisory authority shall deal with requests and complaints lodged by data subjects concerning their data protection rights and shall keep data subjects informed of progress.

4. The supervisory authorities shall act with complete independence and impartiality in performing their duties and exercising their powers and in doing so shall neither seek nor accept instructions.

5. Each Party shall ensure that the supervisory authorities are provided with the resources necessary for the effective performance of their functions and exercise of their powers.

5bis. Each supervisory authority shall prepare and publish a periodical report outlining its activities.

1. Investigación e intervención.
2. Funciones referidas a los flujos transfronterizos de datos (descritas en el artículo 12), en particular la aprobación de las garantías estandarizadas.
3. Toma de decisiones con respecto a las violaciones del Convenio e imposición de sanciones administrativas.
4. Legitimación para participar en procedimientos judiciales o denunciar ante las autoridades judiciales competentes las violaciones del Convenio.
5. Promover el conocimiento público de sus funciones, de sus competencias y de sus actividades; promover también la conciencia pública sobre los derechos de los interesados y el ejercicio de tales derechos, así como la concienciación por parte de los responsables y encargados del tratamiento de sus obligaciones respecto del Convenio; y todo ello con especial atención a los derechos de los niños y de las personas vulnerables.

Establece también el borrador del nuevo texto que todos las Autoridades de supervisión de los Estados miembros tendrán que ser consultadas sobre las propuestas legislativas o medidas administrativas que prevean un tratamiento de datos personales, así como hacer frente a las peticiones y denuncias formuladas por los interesados manteniéndolos informados.

Cuestión especialmente relevante es la que atañe a la independencia de estos órganos. Deberán actuar con total independencia e imparcialidad en el desempeño de

5ter. Members and staff of the supervisory authorities shall be bound by obligations of confidentiality with regard to confidential information they have access to or have had access to in the performance of their duties and exercise of their powers.
6. Decisions of the supervisory authorities may be appealed against through the courts.
7. In accordance with the provisions of Chapter IV, the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties and exercise of their powers, in particular by:
a. providing mutual assistance by exchanging relevant and useful information and cooperating with each other under the condition that, as regards the protection of personal data, all the rules and safeguards of this Convention are complied with;
b. coordinating their investigations or interventions, or conducting joint actions;
c. providing information and documentation on their law and administrative practice relating to data protection.
7bis. The information referred to in paragraph 7 littera a shall not include personal data undergoing processing unless such data are essential for co-operation, or where the data subject concerned has given explicit, specific, free and informed consent to its provision.
8. In order to organise their co-operation and to perform the duties set out in the preceding paragraphs, the supervisory authorities of the Parties shall form a network.
9. The supervisory authorities shall not be competent with respect to processing carried out by bodies when acting in their judicial capacity".

sus deberes y en el ejercicio de sus poderes, no solicitando ni aceptando instrucción alguna. Los Estados miembros deberán asegurar que sus Autoridades de control cuentan con recursos necesarios para el desempeño eficaz de sus funciones y el ejercicio de sus competencias, y sus miembros estarán obligados por la confidencialidad.

Las decisiones de las Autoridades de supervisión podrán ser objeto de recurso ante los tribunales, lo cual acrecienta la garantía en un Estado de Derecho, además de publicar un informe periódico en el que describan sus actividades.

Las Autoridades de control deberán cooperar entre si prestándose asistencia mutua en cuanto a información –siempre desde el cumplimiento del Convenio-, coordinación de sus investigaciones y acciones conjuntas.

Es importante señalar como gran novedad que aporta este nuevo texto y siempre en línea con el nuevo Reglamento General de Protección de Datos y con la política de protección de datos llevada a cabo en la Unión Europea, la obligación de formar una red de Autoridades, que sería una figura similar al Grupo de Trabajo del Artículo 29.

En lo que al Comité Consultivo del Convenio 108 se refiere, el borrador presentado por el Comité CAHDATA, lo dota de nuevas competencias que analizaremos más adelante[55].

A la vista del análisis de las novedades presentadas (si bien aún bajo formato de borrador), son claros los esfuerzos por generar una interoperabilidad del Convenio 108 y el nuevo Reglamento General de Protección de Datos que mejore la relación entre el derecho fundamental a la protección de datos y el desarrollo tecnológico. Tal y como exponía María *Michaelidou*[56] en su presentación, los beneficios para las empresas y los negocios vendrán de la mano de las Autoridades de control, de la confianza del usuario, y de una mayor seguridad con la evaluación de los riesgos.

[55] Apartado 2.4.1.1.
[56] *Michaelidou.* Ver 45.

2.1.3 Jurisprudencia del Tribunal de Derechos Humanos del Consejo de Europa.

La jurisprudencia en materia de protección de datos de carácter personal en el Tribunal de Derechos Humanos del Consejo de Europa (TEDH) ha sido bastante desarrollada, interpretando el derecho al respecto a la vida privada en sentido amplio[57]. El TEDH ha ido definiendo en el trascurso de su jurisprudencia a este derecho como autónomo y diferenciado del derecho a la intimidad.

Así ocurrió en el caso Gaskin[58], donde un ciudadano inglés deseaba conocer datos de las familias de acogida por las que había pasado en su infancia. El Tribunal sentenció que se había conculcado el artículo 8 del Convenio Europeo de Derechos Humanos, ya que los expedientes sobre la historia de una persona son parte de su vida privada y familiar y que en base al Convenio se debería proteger su derecho a recibir dicha información. Sin embargo, también alude a las restricciones que los Estados miembros pueden establecer en caso de negativa de los padres biológicos a revelar sus datos, debiendo existir en estos casos una autoridad u organismo independiente que decida sobre el conflicto, reconociendo en la sentencia que el acceso a esos datos quedaba amparado por el artículo 8 CEDH.

Con mayor contundencia, en el caso Z. vs Finlandia, el TEDH determinó que la protección de los datos personales *"tiene una importancia fundamental para el disfrute por una persona de su derecho al respeto de la vida privada y familiar garantizado en el artículo 8 del Convenio"*[59].

En el asunto CC vs España, y en relación a la publicación de datos personales en una sentencia, el TEDH declaró que "*la publicación de la identidad del demandante en la sentencia en cuestión, ha atentado contra su derecho a su vida privada y familiar, garantizado por el artículo 8 del Convenio*"[60].

---

[57] STEDH A 116 *Leander* v. Suecia, de 26 de marzo de 1987.

[58] STEDH A 160 *Gaskin* v. Reino Unido, de 7 de julio de 1989.

[59] STEDH Z v. Finlandia, de 25 de Febrero de 1997.
También se hace alusión, aunque en otros términos, a la ponderación de los derechos, ya que el tribunal establece que en las cuestiones relativas al acceso por el público a datos personales, las autoridades nacionales gozan de un «margen de apreciación» para sopesar el alcance de la reserva de los datos personales, que depende de diversos factores, como la naturaleza o entidad de los intereses en juego y la gravedad de la interferencia.

[60] STEDH C.C vs España, de 6 de octubre de 2010. En este caso, donde se demandaba a una compañía de seguros por no querer pagar una indemnización por incapacidad, el demandante alega

En 2013, el Consejo de Europa hizo público un documento que contenía una lista con todos los casos juzgados por el Tribunal Europeo de Derechos Humanos en materia de protección de datos, así como su correspondiente resumen, documento muy completo a efectos de estudio de la jurisprudencia[61].

2.2 Directrices internacionales.

2.2.1 La Organización para la Cooperación y el Desarrollo Económicos (OCDE).

La OCDE nace al igual que otras instituciones (como la ONU o El Consejo de Europa) en la estela dejada por la II Guerra Mundial, con un objetivo claro de mejorar la vida y las relaciones entre los países evitando que una nueva guerra pudiera llegar. *"Sus raíces surgen de los escombros de la Segunda Guerra Mundial. Decididos a evitar los errores de sus predecesores a raíz de la Primera Guerra Mundial, los líderes europeos se dieron cuenta de que la mejor manera de garantizar una paz duradera era fomentar la cooperación y la reconstrucción , en lugar de castigar a los vencidos".*[62]

La Organización Europea de Cooperación Económica (OECE), origen de la actual OCDE, surge en 1948 para llevar a cabo el Plan Marshall financiado por Estados Unidos para reconstruir Europa. A la vista del éxito obtenido en la cooperación del continente donde sus miembros se reconocen la interdependencia en sus economías, Canadá y EEUU decidieron unirse al "club" y firmaron un nuevo convenio el 14 de diciembre de 1960, creando la OCDE de nuestros días, entrando en vigor el 30 de septiembre de 1961. En 1964 se uniría también Japón, y así hasta llegar a los 34

que el derecho a su vida privada ha sido violado por el hecho de la divulgación de su identidad con respecto a su estado de salud, en el juicio pronunciado en primera instancia respecto a su persona, para lo que invoca el artículo 8 del Convenio. El TEDH concluyó que sí había existido tal violación.

[61] Disponible en: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/DP%202013%20Case%20Law_Eng%20(final).pdf.

[62] Disponible en: http://www.oecd.org/about/history/.

miembros actuales[63]. La UE tiene el estatus de Observador en el Consejo con voz pero sin voto. Junto a los miembros existen unos socios clave, los llamados *"key partners",* que son Brasil, India, Indonesia, República Popular de China y Sudáfrica. Estos 39 países suponen el 80% mundial del comercio y de la inversión.

La labor de la OCDE consiste en ser supervisores constantes de la realidad de los países, obteniendo así abundante información sobre temas muy diversos que afectan a la sociedad, para posteriormente analizarla, debatirla en los Comités y adoptar decisiones en forma de Recomendaciones que después los países deberán implementar, existiendo un seguimiento posterior por parte de los miembros.

Los informes y análisis realizados por la OCDE aportan amplia información acerca de lo que ocurre en gran parte del mundo, evalúan constantemente la realidad y por ende, sus recomendaciones tienen una base fáctica tan importante que se hace imprescindible tenerlas en cuenta. Sus directrices son de aplicación en países con sistemas jurídicos muy distintos, y, en lo que a nuestro estudio concierne, países como EEUU o los pertenecientes a la Unión Europea suscriben y confluyen en ellas.

Como no podía ser de otra forma, la protección de datos ha sido una de las temáticas abordadas por este organismo. En 1969, la OCDE inició unos estudios sobre la utilización de los ordenadores en el sector público, dando lugar al programa sobre los flujos de datos transfronterizos que más tarde serían la base de las directrices sobre la privacidad. *"Un Grupo de Expertos, el Jurado/Panel de Banco de Datos, analizó y estudió diferentes aspectos del tema de la privacidad, por ejemplo en relación a la información digital, la administración pública, los flujos de datos transfronterizos y las implicaciones de las políticas en general. Para demostrar la naturaleza de los problemas, el Jurado de Bancos de Datos organizó un Simposium en Viena en 1977 en el que se recogieron opiniones y experiencias de diversos sectores como, entre*

[63]Sobre los miembros y socios, http://www.oecd.org/about/membersandpartners/.
Socios Fundadores: Alemania, Austria, Bélgica, Canadá, Dinamarca, España, Estados Unidos, Francia, Grecia, Irlanda, Islandia, Luxemburgo, Noruega, Países Bajos, Portugal, Reino Unido, Suecia, Suiza, Turquía e Italia (1961). Posteriormente se han incorporado Japón (1964), Finlandia (1969), Australia (1971), Nueva Zelanda (1973), México (1994), República Checa (1995), Corea, Hungría y Polonia (1996), República Eslovaca (2000), Chile, Estonia, Eslovenia e Israel (2010).

otros, el gobierno, la industria, los usuarios de redes de comunicación de datos, los servicios de proceso y organizaciones intergubernamentales interesadas"[64].

2.2.1.1 Directrices sobre protección de la privacidad y flujo transfronterizo de datos. 1980.

Por vez primera, en 1980 dicta las primeras Directrices sobre Protección de la privacidad y flujos transfronterizos de datos personales[65]. Fueron adoptadas como una Recomendación del Consejo de la OCDE apoyando los tres principios que aglutinan a los países de la OCDE: democracia pluralista, respeto de los derechos humanos y economías de mercado abiertas. Este documento tiene gran importancia ya que es el primer estudio en profundidad acerca de la protección de datos personales en un ámbito supraestatal.

Los principios básicos de estas Directrices de 1980, a cuya adhesión se recomienda a los Países miembros, son los siguientes:

- Principio de limitación de recogida[66], que establece que debe haber límites en la recogida de los datos y consentimiento del sujeto para ello;
- Principio de calidad de los datos[67], donde los datos deberán ser correctos, completos, actualizados y ser necesarios para los fines para los que se van a usar;

[64] Memoria explicativa Directrices de la OCDE sobre protección de la privacidad y flujo transfronterizo de datos de 1980. Anexo a la Recomendación del Consejo, de 23 de septiembre de 1980.

[65] Disponible en: http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf.
Resumen de las Directrices de la OCDE sobre protección de la privacidad y flujo transfronterizo de datos personales: http://www.oecd.org/sti/ieconomy/15590267.pdf.
OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. © OCDE, 2002.

[66] Punto 7 de las Directrices de la OCDE sobre protección de la privacidad y flujo transfronterizo de datos de 1980. Anexo a la Recomendación del Consejo, de 23 de septiembre de 1980.
"Principio de limitación de recogida. Debería haber límites a la recogida de datos personales y cualquiera de esos datos debería ser obtenido por medios legales y honestos y, en su caso, con el conocimiento o consentimiento del sujeto de los datos".

[67] Punto 8 Directrices OCDE 1980.
"Principio de calidad de los datos. Los datos personales deberían corresponder a los fines para los que se van a usar y, en la medida en que sean necesarios para esos fines, deberían ser correctos y completos, y estar actualizados".

- Principio de especificación de los fines[68], debiendo informar a la recogida de los datos, limitando su uso a esos fines y a otros que no sean incompatibles siempre que se informe al sujeto;
- Principio de limitación del uso[69], es decir no se deben revelar ni usar para fines distintos salvo que se tenga el consentimiento de la persona o exista un imperativo legal;
- Principio de salvaguarda de la seguridad[70], donde se deberán disponer medidas contra riesgos como pérdidas, destrucción, acceso no autorizado, uso, modificación o revelación de datos;
- Principio de transparencia[71], dando a los ciudadanos la posibilidad de conocer sobre el tratamiento, uso y políticas relativos a los datos personales, así como los medios para informar sobre la naturaleza de esos datos, los fines y la identidad del inspector de datos (entendiendo por tal a la persona que decide sobre el uso y finalidad de los datos);
- Principio de participación individual[72], siendo que toda persona tiene derecho a saber si un inspector de datos tiene o no datos suyos y que se le comunique

[68] Punto 9 Directrices OCDE 1980.
"Principio de especificación de los fines. Los fines para los que los datos personales se recogen deberían especificarse en el momento en que se recogen, y su uso posterior estaría limitado al cumplimiento de esos fines o de otros que no sean incompatibles con esos fines y se especifiquen cada vez que haya un cambio de fines".

[69] Punto 10 Directrices OCDE 1980.
"Principio de limitación de uso. Los datos personales no se deberían revelar, poner a disposición del público ni usar para fines que no sean los especificados de conformidad con el apartado 9 anterior, excepto:
a) con el consentimiento del sujeto de los datos; o
b) por imperativo legal".

[70] Punto 11 Directrices OCDE 1980.
"Principio de salvaguarda de la seguridad. Los datos personales deberían estar protegidos por las oportunas medidas de salvaguarda contra riesgos como pérdida o acceso no autorizado, destrucción, uso, modificación o revelación de datos".

[71] Punto 12 Directrices OCDE 1980.
"Principio de transparencia. Debería haber una política general de transparencia en lo concerniente al tratamiento, el uso y las políticas relativos a los datos personales. Se deberían poner los medios para establecer la existencia y la naturaleza de los datos personales, así como los fines principales para los que se van a usar, así como la identidad y el domicilio habitual del inspector de datos".

[72] Punto 13 Directrices OCDE 1980.
"Principio de participación individual. Toda persona física debería tener derecho a: a) conseguir, a través de un inspector de datos o de otra manera, la confirmación de si el inspector tiene o no tiene datos relativos a su persona; b) que se le comunique cualquier dato relativo a ella: en un plazo de tiempo razonable, con una tarifa, en su caso, que no sea excesiva, de manera razonable y de forma que pueda entender fácilmente; c) que se le den las razones de porqué se rechaza una

cualquier dato en un tiempo razonable, con poco coste y de forma comprensible, que se motiven las resoluciones que denieguen el ejercicio de tales derechos y recusar los datos relativos a ellas;

- Principio de responsabilidad[73] hacia el inspector de datos por el cumplimiento de las medidas que permiten la aplicación de los principios.

Adicional a estos principios, establece

- Principios básicos de aplicación internacional sobre el libre flujo y las restricciones legítimas[74], donde hace un llamamiento a la responsabilidad de los países, y a la vez que reclama que ningún país ponga trabas al tránsito de datos exceptuando dicho tránsito para los casos en que el país receptor no respete sustancialmente las Directrices o bien que la re-exportación de esos datos trasgreda su legislación nacional sobre privacidad, abriendo la posibilidad de que los Estados miembros impongan restricciones respecto de ciertas categorías de datos.

Es de resaltar que en dichas Directrices se insta a los Países miembros a establecer procedimientos o instituciones legales, administrativos o de otro tipo para la protección de estos derechos[75], concretando además la obligación de tener una

petición hecha de conformidad con lo establecido en los apartados (a) y (b), y poder recurrir ese rechazo; d) recusar los datos relativos a ella y, si la recusación tiene éxito, hacer que se eliminen, rectifiquen, completen o modifiquen los datos"

[73] Punto 14 Directrices OCDE 1980.
"Principio de responsabilidad. A todo inspector de datos se le deberían pedir responsabilidades por el cumplimiento de las medidas que permiten la aplicación de los principios antes expuestos".

[74] Puntos 15 a 18 Directrices OCDE 1980.
"Todo País Miembro debería tener en cuenta las implicaciones para los demás Países Miembros del tratamiento nacional y la re -exportación de datos personales.
Los Países Miembros deberían tomar todas las medidas oportunas y razonables para garantizar que los flujos transfronterizos de datos personales, incluido el tránsito a través de un País Miembro, sea ininterrumpido y seguro.
Todo País Miembro debería evitar el restringir los flujos transfronterizos de datos personales entre él y otro País Miembro, excepto si éste último todavía no respeta sustancialmente estas Directrices o si la re-exportación de esos datos pudiera transgredir su legislación nacional sobre privacidad. Pero un País Miembro puede imponer restricciones respecto de ciertas categorías de datos personales para los que su legislación doméstica sobre privacidad contempla normas concretas dictadas por la naturaleza de esos datos, y para los que los demás Estados Miembros no tienen prevista una protección similar.
Los Países miembros deberían evitar el elaborar leyes, políticas y prácticas en nombre de la protección de la privacidad y las libertades individuales que pudieran crear obstáculos a los flujos transfronterizos de datos personales que se excedieran en requisitos para esa protección".

[75] Punto 19 Directrices OCDE 1980.

normativa nacional adecuada, fomentar la autorregulación, facilitar los medios para que las personas ejerzan sus derechos, garantizar que no haya discriminación desleal contra los sujetos y establecer un sistema de sanciones y soluciones para el caso de incumplimiento.

2.2.1.2 Declaración sobre flujos de datos transfronterizos. 1985.[76]

El 11 de abril de 1985 los ministros de la OCDE adoptaron la Declaración sobre flujos de datos transfronterizos, que abordaba los temas políticos surgidos por el flujo de datos Personales, tales como actividades comerciales, flujos entre empresas, servicios de información, e intercambios científicos y tecnológicos.

Con esta Declaración los países miembros de la OCDE reafirmaron el compromiso de buscar soluciones armonizadas ante los nuevos retos del flujo de datos que se planteaban en ese momento.

2.2.1.3 Declaración ministerial sobre la protección de la privacidad de las redes globales. 1998.[77]

El compromiso de los miembros de la OCDE sobre la protección de la privacidad de las redes globales para garantizar el respeto a los derechos de los ciudadanos y evitar restricciones innecesarias en los flujos de datos personales fue ratificado en la Conferencia Ministerial de la OCDE "Un mundo sin fronteras: determinación del potencial del comercio electrónico", que se celebró en 1998 en Ottawa.

"Al implantar a nivel nacional los principios establecido en las Partes Segunda y Tercera, los Países Miembros deberían establecer procedimientos o instituciones legales, administrativos o de otro tipo para la protección de la privacidad y las libertades individuales en relación con los datos personales. Los Países miembros deberían ocuparse en especial de:
a) aprobar la legislación nacional adecuada;
b) fomentar y respaldar la autorregulación, bien en forma de códigos de conducta o de otra manera;
c) facilitar los oportunos medios para que las personas físicas puedan ejercer sus derechos; d) procurar las oportunas sanciones y soluciones en caso de incumplimiento a través de medidas que pongan en práctica los principios establecidos en las Partes Segunda y tercera; y e) garantizar que no haya discriminación desleal contra los sujetos de los datos".

[76] OCDE. C(85)139.

[77] Declaración Ministerial de 8-9 de Octubre de 1998 [C(98)177(Anexo 1)].

En esta Conferencia, los Ministros declararon que *"trabajarían para vincular los diferentes enfoques adoptados por los países miembros con vistas a asegurar la protección de la privacidad en las redes globales basándose en las directrices de privacidad de la OCDE"*, reafirmando el compromiso que ya habían adquirido desde 1980.

2.2.1.4 Revisión de las Directrices sobre la Privacidad. 2013.[78]

En 2008 los Ministros de la OCDE, reunidos en la Conferencia de Seúl, acordaron hacer una Declaración para el futuro de la economía de Internet a fin de evaluar las directrices vigentes en materia de protección de la privacidad y de los flujos transfronterizos de datos de carácter personal que acabamos de analizar. Se comprometieron a su análisis previo estudio del cambio existente en la tecnología tanto para los mercados como para los usuarios.

En 2011 se reunió el Grupo de Trabajo de la OCDE sobre la Seguridad de la Información y Privacidad (WPISP[79]) para comparar la situación de aquel momento con la de los años 80, constatando cambios profundos en el valor de los datos personales en la economía, en la sociedad actual y en nuestras propias vidas. Cambios tales como el volumen de datos de carácter personal que se recogen, usan y almacenan; los distintos tipos de análisis de datos que pueden proporcionar perfiles de individuos o grupos; los beneficios sociales y económicos que se obtienen con los nuevos usos y las nuevas tecnologías; la magnitud de las amenazas a la privacidad; la cantidad de actores que intervienen pudiendo poner en riesgos la protección de la privacidad; la frecuencia y complejidad de las interactuaciones personales y la disponibilidad global de datos de carácter personal, el apoyo de redes y plataformas que permiten el continuo flujo de datos.

[78] http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
[79] *Working Party on Information Security and Privacy*.

El WPISP convocó a todos los sectores interesados – grupo de expertos[80]- antes de la aprobación definitiva por el Consejo de la OCDE, y finalmente adoptó una Recomendación revisada respecto de las Directrices sobre la Privacidad[81].

Las nuevas directrices tienen dos líneas básicas sobre las que pivotan sus contenidos: la gestión de riesgos y la interoperabilidad. Si bien mantienen intactos los principios básicos de 1980 incluye además nuevos e importantes conceptos tales como:

- la notificación de las brechas de seguridad, tanto a una autoridad de control como a los sujetos afectados;
- el principio de responsabilidad o rendición de cuentas -la *"accountability"* inglesa-, lo cual supone que los responsables del tratamiento adopten programas efectivos de cumplimiento de la normativa para poder gestionar mejor el riesgo;
- el cumplimiento -*"enforcement"*-.

Hemos de resaltar aquí que es la primera vez que la OCDE reconoce las Autoridades de control[82], como un organismo público establecido por cada país miembro y que será responsable del cumplimiento de la normativa de protección de datos, a las que les reconocen el poder de investigar así como de ejecutar las normas.

La OCDE, organismo preocupado por el desarrollo económico y social, hace especial énfasis en la importancia del flujo transfronterizo de datos por ser fuente de progreso y economía, y asume y se adapta a la nueva realidad del *cloud computing*[83]. Por ello la OCDE, en aras a facilitar el flujo internacional de los datos incide sobre la responsabilidad *("accountability")* del responsable del tratamiento,

[80] Representantes de los gobiernos, autoridades de control, miembros de la sociedad civil, de los negocios y de internet.

[81] *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (2013). [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79]

[82] Se recoge la definición en el punto 1 d) de la parte primera del Anexo de las Directrices para la protección de la privacidad y la transferencia de datos personales de 2013: *"Privacy enforcement authority means any public body, as determined by each Member country, that is responsible for enforcing laws protecting privacy, and that has powers to conduct investigations or pursue enforcement proceedings"*.

[83] *Cloud computing*, también conocido como servicios en la nube, es una programación que permite ofrecer servicios a través de una red, que suele ser internet.

independientemente de si su sistema jurídico está basado en normas adecuadas para la protección o usa medidas corporativas vinculantes tales como las *Binding Corporate Rules* (BCR)[84] o las reglas de privacidad transfronterizas, las *Cross Border Privacy Rules* (CBPR)[85].

Cuestión también relevante en estas recientes Directrices es la referencia a la cultura en materia de protección de datos que los Estados deben potenciar y que compartimos profundamente, pues no existirá sistema que funcione mientras que los ciudadanos no lo conozcan en profundidad y forme parte de sus vidas.

En las líneas anteriormente descritas, el nuevo Reglamento General de Protección de Datos[86] incorpora también estos nuevos principios y está en consonancia con las Directrices de la OCDE.

El análisis pormenorizado de los principios expuestos nos llevan una vez más a sugerir la idoneidad de suscribir el Convenio 108 del Consejo de Europa por parte de EEUU, y ello además de por todas las razones expuestas anteriormente, porque este país es miembro fundador de la OCDE, miembro muy activo y con gran influencia en la organización[87], y acepta sus directrices. Los principios descritos en estas Directrices coinciden plenamente con el contenido del derecho fundamental recogido en los distintos instrumentos europeos, tales como el Convenio 108, la Carta de Derecho Fundamentales o la Directiva 95/46/CE: consentimiento, información, control, calidad, lealtad, seguridad y confidencialidad.

[84] Las ("BCR")- Normas corporativas vinculantes- son normas internas, como códigos de conducta, adoptadas por un grupo multinacional de empresas que definen su política global con respecto a las transferencias internacionales de datos personales dentro del mismo grupo de sociedades ubicadas en países que no proporcionan un nivel adecuado de protección. Son un marco de cumplimiento de la privacidad constituido por un contrato vinculante, procesos y políticas comerciales, formación y directrices que han sido aprobados por las autoridades de protección de datos de la mayor parte de los estados miembros de la UE.

[85] Las Reglas Transfronterizas de Privacidad (CBPR) es un sistema de reglas acerca de la privacidad en el flujo transfronterizo de datos en el área de la APEC.
Para mayor detalle, http://www.cbprs.org/GeneralPages/About.aspx.

[86] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) - 2012/0011 (COD).

[87] En 2015 EEUU ha aportado el 21% de la financiación de la OCDE, según consta en la página web de la organización: http://www.oecd.org/about/budget/.

2.2.2 El Foro de Cooperación Económica Asia-Pacífico (APEC).

La APEC es un foro económico que reúne a 21 países de las áreas de Asia y del Pacífico[88], cuyo objetivo principal es apoyar el desarrollo económico en la zona.

2.2.2.1 Marco de Privacidad de 2004.

Alineándose con las Directrices de la OCDE, en 2004 los Ministros del Área APEC, reconociendo la importancia de la protección de la privacidad y que ésta pudiera ser obstáculo al flujo de información, aprobaron un Marco de Privacidad[89] que facilitara el comercio y la seguridad a los consumidores, alegando 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 de los miembros obtengan todos los beneficios del comercio electrónico[90]. La protección de datos aparece como consecuencia del libre comercio.

Establece el Marco de Privacidad que los sujetos objetos de protección serán solamente las personas físicas.

Los principios básicos de este Marco de Privacidad traídos al documento desde las Directrices de la OCDE son los siguientes[91]:

- Prevención de daños.
- Aviso (Información).
- Límites a la recolección (a datos relevantes para la finalidad).

[88] Son miembros de APEC: Australia, Brunei Darussalam, Canadá, Chile, República Popular de China, Hong Kong (China), Indonesia, Japón, República de Corea, Malasia, México, Nueva Zelanda, Papúa Nueva Guinea, Perú, Las Filipinas, Rusia, Singapur, Taipei Chino, Thailandia, EEUU y Vietnam. Mayor detalle en http://www.apec.org/About-Us/About-APEC/Member-Economies.aspx.

[89] Marco de Privacidad de la APEC de 2005. ISBN 981-05-4471-5.
Para mayor detalle consultar: http://publications.apec.org/publication-detail.php?pub_id=390.

[90] Idem. Página 2.

[91] Marco de Privacidad de 2005. Parte II.

- Usos de la información personal (sólo para la finalidad otorgada y otras compatibles, con excepciones).
- Elección (mecanismos a los individuos para que decidan sobre sus datos cuando sea apropiado).
- Integridad de la información personal (datos exactos y actualizados).
- Medidas de seguridad.
- Acceso y corrección.
- Responsabilidad (por parte del controlador de la información, equivalente al responsable del tratamiento).

Estos principios están diseñados para que cada economía lo aplique según su sistema legal.

El Marco de Privacidad de la APEC promueve además la creación de instrumentos internacionales que protejan la privacidad de los ciudadanos permitiendo el intercambio de información entre los países. Destaca como uno de esos instrumentos el Sistema de Reglas de Privacidad Transfronteriza (CBPR). Este sistema facilita la transferencia de datos de forma segura. Su sistema de control es piramidal con cuatro niveles: Organizaciones, *Accontability agents*, Autoridades de Privacidad y Protección de datos y Subgrupo de Privacidad de Datos y del Panel de Supervisión. Las organizaciones que desean participar del sistema han de someter sus reglas y política de protección de datos a la validación de terceros certificadores (A*ccontability agents),* o Agentes Vigilantes; estos terceros se encuentran validados por Autoridades de Privacidad y Protección de Datos, que son quienes vigilan el funcionamiento correcto en su territorio; y por último, esas Autoridades dependen del Subgrupo de Privacidad de Datos y del Panel de Supervisión, que son quienes realizan las funciones administrativas para mantener el sistema CBPR.

Los Agentes Vigilantes (*Accountability agents*) son aquellas organizaciones públicas o privadas que desempeñan una o ambas de las siguientes funciones: certifican que las CBPR de las empresas siguen el Marco de Privacidad APEC y proporcionan servicios de resolución de conflictos en materia de privacidad entre consumidores y

empresas. Estos agentes pueden ser reguladores como un comisionado de privacidad o bien, autoridades sectoriales como las relativas a la protección del consumidor.
Para que una empresa esté certificada por el sistema APEC CBPR, ésta debe estar sujeta a una economía de un país que participe en el sistema y tener al menos un *Accountability Agent*[92] que ofrezca sus servicios[93].

2.2.2.2 Reglas de Privacidad Transfronteriza 2007.

En el año 2007, los Ministros de la APEC reunidos en Sidney alcanzaron un nuevo acuerdo denominado *"Privacy Pathfinder"* para mejorar el sistema de flujo transfronterizo de datos, cuya finalidad era describir el sistema de CBPR, sus elementos básicos, estructura de gobierno y las funciones y responsabilidades de las organizaciones participantes, instituciones de control y las economías.

2.2.2.3 Grupo de Trabajo APEC-UE.

En 2011 se creó un Comité de Trabajo de la APEC con la Unión Europea[94] para analizar las similitudes y diferencias entre el sistema CBPR y el Sistema de Reglas Corporativas (BCR) de la UE, ya que estos últimos son uno de los mecanismos seleccionados por la UE para permitir el flujo transfronterizo de datos con terceros países. Y en enero de 2014 desarrollaron un documento de referencia común para la estructura ambos sistemas[95]. El objetivo de este documento es servir como una lista de verificación práctica informal para las empresas que soliciten la autorización del Sistema de Reglas Corporativas (BCR) de la UE y la certificación bajo el sistema de Reglas de Privacidad Transfronteriza (CBPR) de la APEC. Además, el documento esboza los requisitos de cumplimiento y certificación de ambos sistemas,

[92] Trust-e es el primer tercero certificador reconocido por APEC: https://www.truste.com/.
[93] Actualmente hay cuatro economías participantes de APEC: EE.UU., México, Japón y Canadá. Para mayor información acerca de las empresas certificadas: http://www.cbprs.org/Business/BusinessDetails.aspx.
[94] El Comité está integrado por las economías de APEC interesadas y representantes de las Autoridades de protección de datos en el Grupo de Trabajo del artículo 29 de la Unión Europea y de la Comisión Europea.
[95] *Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents.* 548/14/EN. WP 212.

especificando los requisitos comunes y los adicionales para cada uno. El objetivo de este Comité de Trabajo es a largo plazo, buscar la interoperabilidad de ambos sistemas, por lo que esta primera iniciativa es sólo un primer paso.

2.2.3 La Organización de las Naciones Unidas (ONU).

La ONU es un organismo internacional que surge, como otros que hemos ido viendo, a raíz de la devastación de la Segunda Guerra Mundial, en 1945[96], y cuya prioridad es mantener la paz y la seguridad internacional y lograr *"la cooperación internacional en la solución de los problemas de carácter económico, social, cultural o humanitario y en el desarrollo y estímulo del respeto a los derechos humanos y las libertades fundamentales de todos, sin distinción por motivos de raza, sexo, idioma o religión"*[97].

Es el organismo internacional que más países del mundo agrupa, casi la totalidad.[98]

2.2.3.1 Directrices para la regulación de los archivos de datos personales informatizados de 1990.[99]

Siendo consciente de la importancia del tráfico de datos de carácter personal[100] y de las consecuencias que ello puede suponer para el desarrollo de la economía de los

[96] Carta de las Naciones Unidas. San Francisco (EEUU), 26 de junio de 1945.
[97] Carta de las Naciones Unidas. Artículo 1.
[98] Actualmente son 193 los miembros de la ONU. Para más información http://www.un.org/es/members/.
[99] Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/organismos_internacionales/naciones_unidas/common/pdfs/D.3BIS-cp--Directrices-de-Protecci-oo-n-de-Datos-de-la-ONU.pdf.
[100] GARCÍA-BERRIO HERNÁNDEZ, T. *Informática y libertades. La protección de datos personales y su regulación en Francia y España*. Ed. Universidad de Murcia, 2003, p. 61 y 62: *"La preocupación por la invasión en la autonomía personal y la concienciación "intelectual" –que no ciudadana, por su desconocimiento inconsciente- de la limitación que esta amenaza supone para el derecho de autodeterminación reconocido a todo individuo, justifica el foco de interés que en el seno de las Naciones Unidas ha recibido en los últimos años del siglo XX la manifestación postmoderna del derecho general de respeto a la intimidad que, en la terminología constitucional española, se ha dado a a conocer como el derecho a la autodeterminación informativa…. El estatuto de normalización rutinaria –como a daily fundamental right -que el fenómeno de protección de datos fue adquiriendo en el seno de las Naciones Unidas a partir de 1990, es el*

estados, en 1990[101] y 1991[102] la Organización de las Naciones Unidas adoptó las Directrices para la regulación de ficheros automáticos de datos personales, (elaboradas por la Subcomisión para la Prevención de la Discriminación y la Protección de Minorías de la ONU).

Estas Directrices son un documento de mínimos, ya que deja a la iniciativa de cada Estado las normas de archivos de datos personales informatizados, convirtiéndose en un instrumento cuyos contenidos son de fácil incorporación a cualquier sistema normativo. Se basa en los principios de legalidad y lealtad, exactitud, especificación de la finalidad, de acceso del interesado, de no discriminación, de la facultad para hacer excepciones, de seguridad, de supervisión y sanciones, de flujo transfronterizo de datos y de aplicación a los ficheros públicos y privados.

Este documento abre la posibilidad de aplicación también a los documentos no automatizados así como a los ficheros de personas jurídicas que contengan datos de personas físicas.

También se refieren estas Directrices al deber de cada país de designar una "*autoridad legalmente competente para supervisar la observancia de estas directrices*"[103], haciendo pues alusión a las Autoridades de control.

2.2.3.2 Resolución sobre el Derecho a la Privacidad en la Era Digital de 2013.[104]

En 2013, a raíz de la revelación de *Edward Snowden* [105]de información confidencial y secreta de las comunicaciones de varios países, Alemania y Brasil impulsaron una Resolución sobre "el derecho a la privacidad en la era digital" que fue aprobada por la Asamblea General de la ONU con el copatrocino de 50 países.

La Resolución insta a los países miembros a que:

reflejo de un proceso de transformación paulatino operado en el seno de la propia nación postmoderna de los Derechos Fundamentales: el respeto a la persona en su rutina diaria.".

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

[102] Resolución de la Asamblea General las Naciones Unidas de 29 de enero de 1991.

[103] Orientación B de las Directrices de Naciones Unidas de regulación de ficheros automáticos de datos personales de 1990.

[104] Resolución de la Asamblea General A/C.3/68/L.45/Rev.1. Disponible en: http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1.

[105] Ver apartado 3.4.1.1.

"a) Respeten y protejan el derecho a la privacidad, incluso en el contexto de las comunicaciones digitales;
b) Adopten medidas para poner fin a las violaciones de esos derechos y creen las condiciones necesarias para impedirlas, como cerciorarse de que la legislación nacional pertinente se ajuste a sus obligaciones en virtud del derecho internacional de los derechos humanos;
c) Examinen sus procedimientos, prácticas y legislación relativos a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales, incluidas la vigilancia, interceptación y recopilación a gran escala, con miras a afianzar el derecho a la privacidad, velando por que se dé cumplimiento pleno y efectivo de todas sus obligaciones en virtud del derecho internacional de los derechos humanos;
d) Establezcan o mantengan mecanismos nacionales de supervisión independientes y efectivos capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado."[106]

A raíz de esta Resolución sobre el Derecho a la Privacidad en la Era Digital, el Consejo de Derechos Humanos aprobó el 24 de marzo de 2015[107] una Resolución por la que crea la figura del Relator especial sobre el derecho a la privacidad en la era digital durante un periodo inicial de tres años.

El Relator tiene varias funciones, entre ellas reunir información sobre los marcos, prácticas y retos relacionados con el derecho a la privacidad, formulando recomendaciones para su promoción y protección; determinando obstáculos en estos ámbitos, realizando también propuestas y recomendaciones y presentar finalmente un informe anual al Consejo en la 31° sesión (en el 2016) y a la Asamblea General en la 71° (en el 2017/2018), que incluya "observaciones importantes" sobre cómo garantizar este derecho fundamental.

[106] Punto 4 de la Resolución A/C.3/68/L.45/Rev.1.
[107] Resolución de la Asamblea General. A/HRC/28/L.27
http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_28_L27.pdf

2.2.4 Los Estándares Internacionales de la Resolución de Madrid de 2009.[108]

En el año 2009, Las Autoridades de Protección de Datos de 50 países reunidas en la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad en Madrid[109] aprobaron la "Resolución de Madrid" de Estándares Internacionales de Privacidad, documento que se preparó a lo largo de un año por un Grupo de Trabajo encabezado por la Agencia Española de Protección de Datos[110].

Esta Resolución es de gran importancia por cuanto es la base de un futuro Convenio universal vinculante y recoge los distintos enfoques de las diferentes legislaciones de los cinco continentes[111].

El objeto del documento 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; y facilitar los flujos internacionales de datos de carácter personal necesarios en un mundo*

[108] Disponible en: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/09-11-05_Madrid_Int_standards_ES.pdf

[109] Madrid, 5 de noviembre de 2009.

[110] Autoridades del Grupo de Trabajo: Comisario Federal de Protección de Datos (Alemania), Comisario de Protección de Datos y Libertad de Información de Berlín (Alemania), Comisario de Protección de Datos de Schleswig-Holstein (Alemania), Comisión de Protección de Datos (Austria), Comisión de Protección de la Privacidad (Bélgica), Comisión de la Informática y las Libertades (Burkina-Fasso), Comisario de Privacidad (Canadá), Comisario de Acceso a la Información (Canadá), Supervisor Europeo de Protección de Datos, Comisario de Información (Eslovenia), Agencia Española de Protección de Datos (España), Agencia Catalana de Protección de Datos (España), Agencia de Protección de Datos de la Comunidad de Madrid (España), Agencia Vasca de Protección de Datos (España), Comisión Nacional de la Informática y las Libertades (Francia), Comisario de Privacidad para la Protección de Datos (Hong Kong), Comisario de Protección de datos (Irlanda), Garante para la Protección de los Datos Personales (Italia), Comisario de Privacidad (Nueva Zelanda), Comisión de Protección de Datos (Países Bajos), Comisión Nacional de Protección de Datos (Portugal), Comisario de Información (Reino Unido), Oficina para la Protección de Datos Personales (República Checa), Comisario Federal de Protección de Datos (Suiza).

[111] Al respecto, BLAS, F. *Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales*. Derecho del Estado. Núm. 23, 2009, p. 37-66.

globalizado"[112]. Para ello aporta cinco definiciones imprescindibles, tales como dato de carácter personal, tratamiento, interesado, persona responsable y prestador de servicios de tratamiento[113].

La resolución aprobada define un conjunto de principios, derechos y obligaciones que cualquier sistema jurídico que quiera proteger la privacidad debe esforzarse por alcanzar, tales como:

- Principio de lealtad y legalidad[114], donde los tratamientos deberán realizarse de forma leal, considerándose desleales aquellos que den lugar a una discriminación injusta o arbitraria contra los interesados. Este principio descrito en estos términos cobra especial relevancia cuando nos encontramos actualmente con el gran desarrollo que está teniendo el *"big data"*[115], sistema que permite obtener mucha más información a partir de la cantidad de datos existentes, pudiéndose crear perfiles muy detallados de las personas que se podrán ver inmersas en procesos de discriminación de la índole descrita. Las Autoridades de control de Protección de Datos han dicho que: "*el debilitamiento de los principios clave de privacidad, junto con un mayor uso del Big Data, es probable que tenga consecuencias adversas para la protección de la privacidad y de otros derechos fundamentales*"[116].

[112] Artículo 1 Resolución de Madrid.

[113] Artículo 2 Resolución de Madrid: Definiciones.- *"a. "Dato de carácter personal": cualquier información concerniente a una persona física identificada o que pueda ser identificada a través de medios que puedan ser razonablemente utilizados. b. "Tratamiento": cualquier operación o conjunto de operaciones, sean o no automatizadas, que se aplique a datos de carácter personal, en especial su recogida, conservación, utilización, revelación o supresión. c. "Interesado": persona física cuyos datos de carácter personal sean objeto de tratamiento. d. "Persona responsable": persona física o jurídica, de naturaleza pública o privada que, sola o en compañía de otros, decida sobre el tratamiento. e. "Prestador de servicios de tratamiento": persona física o jurídica, distinta de la persona responsable, que lleve a cabo un tratamiento de datos de carácter personal por cuenta de dicha persona responsable".*

[114] Artículo 6 Resolución de Madrid. 2009: *"1. Los tratamientos de datos de carácter personal se deberán realizar de manera leal, respetando la legislación nacional aplicable y los derechos y libertades de las personas, de conformidad con lo previsto en el presente Documento y con los fines y principios de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos. 2. En particular, se considerarán desleales aquellos tratamientos de datos de carácter personal que den lugar a una discriminación injusta o arbitraria contra los interesados".*

[115] El *Big data* es una tecnología que permite analizar grandes cantidades de datos de una forma rápida y eficaz de fuentes muy diversas.

[116] Resolución *Big Data*. 36ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. Mauricio, Octubre de 2014.

- Principio de finalidad[117]. Los datos solo podrán ser usados para la finalidad para la cual se recogen u otra compatible. El proyecto del nuevo Reglamento General de Protección de Datos apunta también en la línea anterior: finalidades compatibles.
- Principio de proporcionalidad[118], pues los datos recabados deberán ser los adecuados, relevantes y no excesivos.
- Principio de calidad[119], debiendo ser los datos exactos, completos y actualizados, y ser cancelados o convertidos en anónimos cuando dejen de servir para la finalidad para la que se recabaron.
- Principio de transparencia[120], el cual incluye la obligación del responsable de facilitar información al ciudadano sobre la identidad del responsable, la finalidad de la recolección o destinatarios a los que se prevé cederle los datos.
- Principio de responsabilidad[121], sobre el que se asienta la obligación de adoptar medidas necesarias para el cumplimiento de la normativa nacional y dotarse de mecanismos para ello.

Para mayor información del contenido:
http://www.privacyconference2014.org/media/16724/Resoluci%C3%B3n-Big-Data.pdf.

[117] Artículo 7 Resolución de Madrid 2009: *"1. El tratamiento de datos de carácter personal deberá limitarse al cumplimiento de las finalidades determinadas, explícitas y legítimas de la persona responsable. 2. La persona responsable se abstendrá 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".*

[118] Artículo 8 Resolución de Madrid 2009: *"1. El tratamiento de datos de carácter personal deberá circunscribirse a aquéllos que resulten adecuados, relevantes y no excesivos en relación con las finalidades previstas en el apartado anterior. 2. En particular, la persona responsable deberá realizar esfuerzos razonables para limitar los datos de carácter personal tratados al mínimo necesario".*

[119] Artículo 9 Resolución de Madrid 2009: *"1. La persona responsable deberá asegurar en todo momento que los datos de carácter personal sean exactos, así como que se mantengan tan completos y actualizados como sea necesario para el cumplimiento de las finalidades para las que sean tratados. 2. La persona responsable deberá limitar el periodo de conservación de los datos de carácter personal tratados al mínimo necesario. De este modo, cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades que legitimaron su tratamiento deberán ser cancelados o convertidos en anónimos".*

[120] Artículo 10 Resolución de Madrid 2009: *"1. Toda persona responsable deberá contar con políticas transparentes en lo que a los tratamientos de datos de carácter personal que realice se refiere…".*

[121] Artículo 11 Resolución de Madrid 2009: *"La persona responsable deberá: a. adoptar las medidas necesarias para cumplir con los principios y obligaciones establecidos en el presente Documento y en la legislación nacional aplicable, y b. dotarse de aquellos mecanismos necesarios para evidenciar dicho cumplimiento, tanto ante los interesados como ante las autoridades de supervisión en el ejercicio de sus competencias, conforme a lo establecido en el apartado 23".*

La Resolución presta también atención a la necesidad del consentimiento del individuo y las posibles situaciones que lo excepcionarían, así como una definición de lo que son datos sensibles y la existencia de garantías adicionales. Por otro lado explica cómo ha de ser la relación con los prestadores de tratamiento.

En cuanto a las transferencias internacionales permite que éstas se realicen cuando el estado al que se transfieran tenga el mismo nivel de protección que se prevé en la Resolución, y que en caso contrario se realicen en determinadas situaciones y cuando las Autoridades de supervisión así lo acuerden.

También define la Resolución los derechos de los interesados, a saber, derecho de acceso, rectificación y cancelación, y derecho de oposición; y en cuanto a la seguridad obliga tanto al responsable como a los prestadores de servicios de tratamiento a la confidencialidad[122] y a *"proteger los datos de carácter personal que sometan a tratamiento mediante aquellas medidas técnicas y organizativas que resulten idóneas en cada momento para garantizar su integridad, confidencialidad y disponibilidad*"[123].

Para asegurar el cumplimiento de estas medidas, el documento obliga a los Estados miembros a ser proactivos estableciendo procedimientos destinados a prevenir y detectar infracciones, designar oficiales de privacidad o protección de datos con cualificación, recursos y competencias suficiente, programas de concienciación social, auditorías, privacidad por o desde el diseño (en inglés, *privacy by design*) y por defecto (*privacy by default*), estudios de impacto previos, adhesión a acuerdos de autorregulación e implementación de planes de contingencias.

En cuanto a las autoridades de supervisión *"deberán ser imparciales e independientes, y contarán con la cualificación técnica, las competencias suficientes y los recursos adecuados para conocer de las reclamaciones que le sean dirigidas por los interesados, y para realizar las investigaciones e intervenciones que resulten*

[122] Artículo 21 Resolución de Madrid 2009.
[123] Artículo 20 Resolución de Madrid 2009.

necesarias para garantizar el cumplimiento de la legislación nacional aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal".[124]

Son estos Estándares Internacionales un paso muy avanzado en aras de conseguir una mayor protección universal del derecho a la protección de datos[125]. En apoyo de esta mejor coordinación global de los distintos marcos de privacidad, diez grandes empresas multinacionales[126] firmaron una declaración de apoyo al desarrollo de sistemas que la permitan. Tal y como señalaba Artemi Rallo[127] estos estándares son una propuesta de mínimos internacionales que recogen un conjunto de principios y derechos que permitan alcanzar el mayor grado de consenso internacional y que sirvan de referencia a los países que no gozan de un marco legal e institucional de protección de datos. Esto es lo que algunos llaman el *"soft law"*.

Del análisis de la Resolución vemos cómo los estándares aprobados realmente pueden ser comunes a casi todos los países. El impacto de éstos ha sido muy positivo, pues de hecho la revisión de las Directrices de Privacidad de la OCDE de 2013, la del Convenio 108 del Consejo de Europa, el proyecto de Reglamento de Protección de Datos de la Unión Europea, y los cambios en la normativa de la APEC (recordemos la existencia del Grupo de Trabajo APEC-UE) se deben en gran medida a este trabajo, y todos ellos coinciden en gran medida.

[124] Artículo 23.2 Resolución de Madrid 2009.

[125] Acerca de la privacidad e internet, CRUCES BLANCO, E. *El ojo que todo lo ve, el control cibernético de la privacidad: Las ventanas y puertas de la intimidad están abiertas.* Boletín ACAL núm. 89, 2013, p. 5-11.

[126] Oracle, Walt Disney, Accenture, Microsoft, Google, Intel, Procter & Gamble, General Electric, IBM y Hewlett-Packard.

[127] Declaraciones en el Diario El Economista.es el 6.11.2009.
Disponible en http://www.eleconomista.es/seleccion-ee/noticias/1675918/11/09/Aprobados-unos-estandares-internacionales-sobre-proteccion-de-datos.html.
ARTEMI RALLO fue Director de la Agencia Española de Protección de Datos (2007-2011).

2.3 La Unión Europea.

2.3.1 Los Derechos Fundamentales en la Unión Europea.

A diferencia del Consejo de Europa que nació para proteger los derechos fundamentales de los ciudadanos en un ámbito de cooperación entre Estados, la Unión Europea surgió en el ánimo de la integración económica de sus países miembros, bajo un paraguas de orden supraestatal[128], en el que todos ellos renunciaban a parte de su soberanía en favor de la Comunidad.[129]

La protección a los derechos fundamentales en el derecho de la Unión (Derecho Comunitario hasta el Tratado de Lisboa de 2009) no se consideró materia necesaria en los inicios de la Comunidad Europea, y ello porque todos los miembros de la Comunidad lo eran a su vez del Consejo de Europa y habían suscrito previamente el Convenio Europeo de Derechos Humanos de 1950. Entendían pues, (tras varios debates en los que se planteó la posibilidad de elaborar un catálogo de derechos fundamentales) que dicha materia estaba suficientemente cubierta. Así se reconoce en 1977 en la Declaración Común del Parlamento Europeo, del Consejo y de la Comisión, en la que *"subrayan la importancia primordial que atribuyen al respecto de los derechos fundamentales que resultan en particular de las constituciones de los*

[128] El inicio de la UE data de 1951, con la creación de la Comunidad Europea del Carbón y del Acero. Tratado CECA. París, 18 de abril de 1951. Miembros: Francia, Italia, Alemania y países del Benelux.
Este Tratado no se publicó en Diario Oficial alguno. Código CELEX 11951K. Entró en vigor el 23/07/1952, y expiró el 23/07/2002, ya que se pactó por un periodo de 50 años.
El 23 de marzo de 1957 estos mismos 6 países firmaron el Tratado de Roma (tampoco publicado) en el que se creó la Comunidad Económica Europea (CEE)- Código CELEX 11957E- y la Comunidad Europea de la Energía Atómica (CEEA) – Código CELEX 11957A-.
Versión actual consolidada de la CEE, DO C 325, de 24.04.2012.
Versión actual consolidada del CEEA, DO C 327 de 26.10.2012.
El 8 de abril de 1965 el Tratado de Bruselas, denominado «Tratado de fusión», supuso la fusión administrativa de las tres organizaciones. DO 152 de 13.7.1967.
Posteriormente se fueron incorporando los demás países a través de distintos Tratados hasta llegar a los 28 actuales.
España se incorporó el 1 de enero de 1986. BOE 1 de enero de 1986, num.1. Tratado de Adhesión de España y Portugal. DO L 302 de 15/11/1985.
El Tratado de Maastricht consagra oficialmente el nombre de "Unión Europea" que en adelante sustituirá al de Comunidad Europea. DO C 191 de 29.7.1992.

[129] DAVARA RODRÍGUEZ, M.A. *La protección de datos en Europa. Principios, derechos y procedimientos*, Universidad Pontificia Comillas, Madrid 1998.

Estados miembros, así como de la Convención Europea de Protección de los Derechos del Hombre y de las Libertades Fundamentales. En el ejercicio de sus competencias y en cumplimiento de los objetivos de las Comunidades Europeas, respetarán y seguirán respetando tales derechos"[130].

Pero el desarrollo económico también supuso (y supone) situaciones en las que las personas pueden ver conculcados sus derechos fundamentales[131]. Y así fue ocurriendo en la recién creada Comunidad Europea. Se fueron sucediendo los casos en los que se solicitaba amparo judicial al propio Tribunal de Justicia de las Comunidades Europeas (TJCE)[132] ante determinados hechos en los que se consideraba que el derecho comunitario era contrario al derecho nacional. Si bien inicialmente el TJCE se declaró incompetente para ello[133] (pues los Tratados no contenían ninguna mención ni catálogo alguno de derechos fundamentales), lo cierto es que se vieron obligados a ir resolviendo dichos asuntos, ante la "*rebelión de los Tribunales constitucionales"*[134], que amenazaban con ser ellos quienes se pronunciasen sobre tales asuntos. La Sentencia *Rutili* fue la primera donde el TJCE entra a valorar sobre la interpretación de una norma en relación a su adecuación a los derechos fundamentales[135], haciendo la primera referencia explícita al CEDH (Convenio Europeo de Derechos Humanos), declarando que éste es *"fuente de inspiración"*. La situación descrita provocó que, a pesar de no tener competencia para dictar sentencias sobre materias referidas a derechos fundamentales, el TJCE lo

[130] DO C 103, DE 27/04/1977.

[131] GALÁN JUÁREZ, M. *La interpretación de los derechos fundamentales por parte del Tribunal Constitucional: una argumentación en términos de razonabilidad*, Isegoría, 2006.

[132] *Artículo 220 del Tratado Constitutivo de la UE (TCE): "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".*

[133] STJCE de 4 de febrero de 1959, caso *Stork.* STJCE de 15 de julio de 1960, caso *Ruhrkohen-Verkaufsgesellschaften.* STJCE de 1 de abril de 1965, caso *Sgarlatta.*

[134] ARENAS RAMIRO, M. Revista Jurídica de Castilla y León, núm. 16, 2008, p.116.

[135] Sentencia *Rutili*, de 28 de octubre de 1975, asunto 36/1975, donde la administración francesa atribuye a un ciudadano italiano –sr. *Rutili*- un permiso de residencia correspondiente a un nacional de un Estado miembro de la CEE, acompañado de una prohibición de residir en determinados departamentos franceses. La sentencia señala que *"un Estado miembro sólo podrá imponer a los nacionales de otros Estados miembros (a los que se aplican las disposiciones del Tratado) medidas restrictivas del derecho de residencia limitadas a una parte del territorio nacional en los casos y en las condiciones en que tales medidas puedan aplicarse a los nacionales del Estado de que se trate".* Ver CORCUERA ATIENZA, J. "La protección de los derechos fundamentales en la Unión Europea: el final de un túnel", en CORCUERA ATIENZA, J. (coord.), *La protección de los Derechos Fundamentales en la Unión Europea*, Dykinson, Madrid, 2002, p. 61-99.

fuera haciendo respecto de todos aquellos asuntos que le iban llegando, creando pues jurisprudencia de forma "pretoriana". Esta jurisprudencia supuso un catálogo propio de derechos fundamentales analizados por el tribunal que tuvo el valor de principios generales del derecho comunitario, tal y como se reconoce en la sentencia del caso *Stauder*.[136]

Se produce en esas sentencias una fusión inicial entre el derecho comunitario y el derecho del Consejo de Europa, yendo este último de la mano del Convenio Europeo de Derechos Humanos,[137] pues el TJCE lo utilizó como *"argumento auxiliar para consolidar soluciones derivadas en primer lugar del propio derecho comunitario, configurando así, a golpe de sentencia, los derechos fundamentales como principios propios del ordenamiento comunitario, extrayéndolos más allá de los Tratados, de las tradiciones constitucionales comunes de los estados miembros y del CEDH*".[138]

A la vista de lo expuesto, se hace importante en este análisis resaltar que el catálogo de derechos fundamentales[139] del Tribunal de Justicia (y que será la base de la actual Carta) se crea no sólo con el contenido del CEDH, sino también con la propia jurisprudencia del Tribunal Europeo de Derechos Humanos así como las tradiciones constitucionales de los países miembros[140].

En 1992, con la firma del Tratado de la Unión Europea (TUE) en Maastricht se avanza en la consecución del reconocimiento de los derechos fundamentales en la

[136] STJCE de 12 de noviembre de 1969, caso *Stauder*.

[137] FREIXES SANJUÁN, T. *Derechos fundamentales en la Unión Europea. Evolución y prospectiva: la construcción de un espacio jurídico europeo de derechos fundamentales*. Revista de Derecho Constitucional Europeo núm. 4, 2005, p. 43-86: *"La postura del TJCE ha sido más fruto del voluntarismo y de su posición militante en defensa de los derechos fundamentales que de las normas comunitarias reguladoras de tales derechos".*

[138] ARENAS RAMIRO,M. Revista Jurídica de Castilla y León, núm. 16, 2008, p.118.
STJCE de 28.10.1975, caso *Rutilli*. Primera referencia explícita al CEDH, afirmando que es *"fuente de inspiración".*

[139] Sobre los distintos proyectos llevados a cabo para la elaboración de un catálogo de derechos fundamentales, ver FREIXES SANJUÁN, T. y REMOTTI, J.C., *El futuro de Europa. Constitución y derechos fundamentales*, Minim Ediciones, Valencia, 2002, p. 12-16; FONSECA MORILLO, F.J., "La gestación y el contenido de la Carta de Niza", en MATIA PORTILLA, F.J. (dir.), *La protección de los derechos fundamentales en la Unión Europea*, Civitas, Madrid, 2002, p. 87-121; y RODRÍGUEZ-VERGARA DÍAZ, A., *Integración europea y derechos fundamentales*, Civitas, Madrid, 2001.

[140] STJCE de 17.12.1970, caso *Internationale Handelsgesellschaft* y STJCE de 14.05.1974, caso *Nold*, donde afirman que la protección de los derechos fundamentales es parte integrante del derecho comunitario, refiriéndose a las tradiciones constitucionales comunes y a los tratados internacionales sobre derechos fundamentales.

Unión Europea.[141] La Unión Europea no pretende ya solamente una unión monetaria y económica, sino una unión en derechos de los ciudadanos comunitarios, donde la libertad, la democracia y los derechos y libertades fundamentales sean la locomotora de su progreso. El artículo 6 del TUE reconoce por vez primera la existencia de estos derechos señalándolos como principios generales del derecho, y conectándolos con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales así como con las tradiciones constitucionales comunes a los Estados miembros.[142]

Pero el espíritu europeo va a más, y desde las propias instituciones se reclama un reconocimiento explícito de los mismos.[143] En el año 2000 se publica la Carta de Derechos Fundamentales para la Unión Europea,[144] la cual es solemnemente proclamada pero carece de valor jurídico, pues no está incorporada a ningún instrumento normativo, ya sea de derecho originario o derivado. Para superar esta situación, se incluyó la Carta en el "Tratado por el que se establece una Constitución para Europa"[145], firmado en Roma en 2004, pasando así a ser derecho originario y estar amparada por el TJCE.

El problema vino cuando la Constitución Europea perdió totalmente su valor al no ser ratificada por algunos estados miembros, tales fueron los casos de Francia y Países Bajos[146]. A pesar de los intentos, la Carta continuaba sin valor jurídico.

[141] Tratado de la Unión Europea (TUE). Maastricht 7 de febrero de 1992. Entra en vigor el 1 de noviembre de 1992. DO C 191 de 29.7.1992.

[142] TUE, art. 6: *"1.-La Unión se basa en los principios de libertad, democracia, respeto de los derechos humanos y de las libertades fundamentales y el Estado de Derecho, principios que son comunes a los estados miembros. 2.- 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".*

[143] Grupo de Expertos. Informe de la Comisión Europea "Afirmación de los Derechos fundamentales en la Unión Europea. Ha llegado el momento de actuar". Febrero 1999.

[144] Carta de Derechos Fundamentales para la Unión Europea. Consejo de Niza, 7 de diciembre de 2000 (DOUE C 364, de 18 de diciembre).

[145] Constitución Europea. DOUE C 310, de 16 de diciembre de 2004.

[146] Resolución del Parlamento Europeo sobre el Tratado por el que se establece una Constitución para Europa, aprobada el 12/01/2005. En ella se recomendaba a los 25 Estados miembros ratificar el Tratado de la Constitución Europea.

Para superar esta situación (que dio origen a una crisis europea y de fomento del euroescepticismo) nuevamente se proclamó solemnemente La Carta de los Derechos Fundamentales[147]y se incluyó en el Tratado de Lisboa de 2007[148], tratado ratificado por todos los países miembros, y por el que los derechos fundamentales pasan por fin a formar parte del Derecho originario europeo y a tener carácter vinculante para los estados miembros. Ello supone que será el TJCE quien ejercite el control sobre los órganos de la Unión y sobre los Estados Miembros. No debemos olvidar que el TJCE no es un Tribunal de Derechos Humanos, sino que su misión es velar por el cumplimiento del ordenamiento comunitario.[149]

2.3.2 El derecho fundamental a la protección de datos de carácter personal.[150]

El reconocimiento de este derecho lleva aparejado un recorrido similar al del resto de derechos fundamentales: nace de la jurisprudencia del TJCE "vía pretoriana" y posteriormente se incorpora específicamente como tal derecho a La Carta de los Derechos Fundamentales recogida en el Tratado de Lisboa de 2007, que modifica el Tratado de la Unión Europea, pasando a formar parte, tal como explicábamos, del

En España fue sometida a referéndum el 20/02/2005, con una mayoría del sí. Ley Orgánica 1/2005, por la que se aprueba el Instrumento de ratificación del Tratado que establece la Constitución Europea. BOE 121, de 21/05/2005.

Al respecto, ver PEDROL, X. *La Constitución Europea y sus mitos*, Icaria, Barcelona, 2005.

147 Carta de los Derechos Fundamentales. DO C 303 de 14/12/2007.

148 Tratado de Lisboa. DO C 306 de 17/12/2007. Entró en vigor el 01/11/2009.

149 BIGLINO CAMPOS, P. *Derechos fundamentales y competencias de la Unión. El argumento de Hamilton*, Revista Derecho Comunitario Europeo. Año 7, núm. 14, enero-abril 2003: "L*os actos de los Estados en los que se excluye las previsiones contenidas en normas de derechos comunitario pueden ser, y de hecho son sometidas al Tribunal de Justicia a través de la vía prejudicial, cuando el juez nacional ad hoc duda de su compatibilidad con el ordenamiento europeo…. El diálogo sobre la validez de la ley ya no se establece sólo entre el juez ad hoc y el Tribunal Constitucional. Este deja de ser el único legitimado para primar de eficacia ese tipo de normas. Ahora son los jueces ordinarios quienes, como guardianes de los derechos fundamentales, inaplican leyes estatales que vulneran esas facultades, utilizando un parámetro distinto a la constitución interna"*

150 Sobre los derechos fundamentales en Europa: ARENAS RAMIRO, M., *El derecho fundamental a la protección de datos personales en Europa*, Tirant lo Blanch, Valencia, 2006; ARNOLD, R. ,"Los derechos fundamentales comunitarios y los derechos fundamentales en las Constituciones nacionales", en MATIA PORTILLA, F.J. (dir.), *La protección de los derechos fundamentales en la Unión Europea*, Cívitas, Madrid, 2002, p. 51-59; CARRILLO, M., "La Unión Europea ante los derechos fundamentales", en VV.AA., *La democracia constitucional. Homenaje al Profesor Francisco Rubio Llorente*, vol. II, Centro de Estudios Políticos y Constitucionales, Madrid, 2002, p. 1407-1422.

derecho originario de la Unión. Pero el recorrido hasta ese punto no está exento de trabas y política[151].

La doctrina coincide en focalizar en el caso *Stauder*[152], 1969, la primera sentencia en la que se reconoce el derecho, no precisamente invocado, a la protección de datos. En ella un ciudadano alemán, sr. *Stauder*, consideró que unas determinadas medidas que había adoptado el gobierno de su país atentaban contra su dignidad. La administración alemana obligaba a revelar sus datos personales a quienes fuesen beneficiarios de unos lotes de mantequilla destinados a personas de un régimen asistencial, ya que dicho alimento procedía de unos excedentes de productos lácteos, y la Comisión Europea autorizó a los Estados miembros a venderla a bajos precios a un sector de población determinada. Con el fin de evitar el fraude, los beneficiarios debían cumplimentar unos cupones con sus datos personales. *Stauder* planteó la cuestión ante un tribunal administrativo de Stuttgart y éste a su vez elevó como cuestión prejudicial al Tribunal de Justicia la posible invalidez de esta Decisión de la Comunidad Europea. El Tribunal de Justicia, si bien no constató violación de derecho, sí manifestó por vez primera que los derechos fundamentales eran principios generales del derecho[153].

Hasta los inicios de los ochenta, hubo distintas iniciativas en relación a la protección de datos. En 1973 un documento interno de la Comisión dirigido al Consejo muestra su preocupación respecto de la privacidad de los ciudadanos en relación al uso de la informática, considerando que se deberían tomar medidas al respecto.[154] En 1974 se

[151] Al respecto, ARENAS RAMIRO, M. *El derecho fundamental a la protección de datos personales en Europa*, Tirant lo Blanch, Valencia, 2006, p. 225-249.

[152] Caso *Stauder*. STJCE de 12 de noviembre de 1969.

[153] Sobre el caso *Stauder*, BALAGUER CALLEJÓN, F., Derecho y derechos en la Unión Europea, en CORCUERA ATIENZA, J. (coord.), *La protección de los derechos fundamentales en la Unión Europea*, Dykinson, Madrid, 2002, p. 39-59; RODRÍGUEZ BEREIJO, A. "La Carta de los derechos fundamentales de la Unión Europea y la protección de los derechos humanos", en FERNÁNDEZ SOLA, N. (coord.), *Unión Europea y Derechos fundamentales en perspectiva constitucional*, Dykinson, Madrid, 2004, p. 11-36. Críticos con estas tesis: RUBIO LLORENTE, F., "Mostrar los derechos sin destruir la Unión", en GARCÍA DE ENTERRÍA, E. (dir.) y ALONSO GARCÍA, R., *La encrucijada constitucional de la Unión Europea*, Cívitas, Madrid, 2002, pp. 113-150.

[154] SEC(73)4300. *"In conclusion, the Commission drew the attention of the Council to the social problems arising from such a policy, and emphasised the need for protection of the private citizen in regard to the development of data processing; it expressed the wish that public hearings should be arranged on the subject".*

elabora un estudio presentado en el Parlamento Europeo el 21 de febrero de 1975 sobre la protección de los derechos de la persona ante el desarrollo de los progresos técnicos en el ámbito de la informática[155] que incentiva a la adopción de una directiva en esta materia, para asegurar a los ciudadanos mejor protección en el tratamiento de sus datos y evitar legislaciones nacionales contradictorias. Avanzando en el tiempo, el 18 de mayo de 1977 se crea la Subcomisión "Informática y derechos de la persona" en el seno de la Comisión Jurídica del Parlamento, y tras numerosas sesiones desde 1978, el 8 de mayo de 1979 el Parlamento aprueba una Resolución por la que se adoptan unas Recomendaciones[156] sobre la protección de los derechos de la persona ante el desarrollo de los progresos técnicos en el ámbito de la informática, las cuales se basaban en el Informe *Bayernl*[157]. Es de destacar en dicho informe la referencia a la regulación de ficheros no automatizados[158].

Si bien es cierto que se realizan todos estos movimientos que denotan la preocupación, no es menos cierto que en la Comunidad se vive un *impass* sin regulación alguna en el que el TJCE se pronuncia sobre demandas presentadas acerca de la protección de datos personales.

Subyace el derecho a la protección de datos en el caso Campogrande[159], donde el Tribunal examina la ausencia del consentimiento en la cesión de datos personales de una funcionaria y su esposo entre Instituciones de las Comunidades Europeas en Bélgica. En el mismo sentido, en el caso X. vs Comisión[160] el Tribunal tiene en cuenta el consentimiento del titular de los datos.

---

155 JO núm. C 60, de 13/03/1975, p. 48. Estudio dirigido por *Lord Mansfield.*

156 Resolución del Parlamento Europeo de 8 de mayo de 1979 sobre la protección de los derechos de la persona ante el desarrollo de los progresos técnicos en el ámbito de la informática. DOC 140, de 05/06/1979.

157 Parlamento Europeo. Documentos de sesión, *Rapport fait au nom de la Commission juridique sur la protection des droits de la personne face au dèveloppement des progres techniques dans le domaine de I'informatique.* Documento 100/79, de 04/05/1979

158 Informe *Bayernl: "No parece existir ninguna razón lógica para excluir los datos personales almacenados y tratados por sistemas manuales, ya que todos los sistemas comprenden ciertos elementos manuales"*.

159 STJCE, Sala Tercera, de 23/04/2002. Caso Campogrande. Anna María Campogrande contra Comisión de las Comunidades Europeas. C -62/01.

160 STJCE, de 05/10/1994. Caso X. contra Comisión. C-404/92. Una persona es sometida a unos análisis médicos para acceder a un empleo en las Comunidades Europeas, donde sin su consentimiento le practicaron la prueba del SIDA. La Comisión utilizó esos datos y no la contrató.

En 1995 se legisla por vez primera en Europa sobre esta materia con 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[161]. Este instrumento normativo incorpora y desarrolla ampliamente el Convenio 108 del Consejo de Europa, cuyos principios se considerarán como un acervo irrenunciable para cualquier regulación de este derecho. La Directiva describirá dichos principios incluso con mayor detalle, ampliando su contenido:

- el principio del consentimiento, no sólo existirá cuando la persona tiene el derecho a cancelar sus datos, sino también en el momento inicial cuando se le recaban los datos[162];
- el principio de información no sólo se dará cuando el individuo solicite información de sus datos, sino también en el momento inicial de la relación, cuando se recojan sus datos[163];
- el principio de control se configura no sólo como el derecho a la rectificación, sino que se crea además el derecho de oposición[164], como un derecho de

[161] Directiva 95/46/CE, de 24 de octubre, 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 (DOCE L 281, de 23 de noviembre).

[162] Artículo 7 Directiva 95/46/CE: "*Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si el interesado ha dado su consentimiento de forma inequívoca, o…* (régimen de excepciones)".

[163] Artículo 10 Directiva 95/46/CE: *"Los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la información que se enumera a continuación, salvo sí la persona ya hubiera sido informada de ello: a) la identidad del responsable del tratamiento y, en su caso, de su representante; b) los fines del tratamiento de que van a ser objeto los datos; c) cualquier otra información tal como: los destinatarios o las categorías de destinatarios de los datos, el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder, la existencia de derechos de acceso y rectificación de los datos que la conciernen"*.

[164] Artículo 14 Directiva 95/46/CE: *"Los Estados miembros reconocerán al interesado el derecho a: a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos; b) oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección , y a que se le ofrezca expresamente el derecho de oponerse , sin gastos, a dicha comunicación o utilización"* .

carácter gratuito. En desarrollo de este principio se crea también un nuevo recurso ante una Autoridad de control independiente[165];

- los principios de calidad y lealtad, estarán presentes obteniéndose y tratándose de forma leal y legítima, registrándose para finalidades determinadas, siendo exactos, adecuados, pertinentes y no excesivos, y durante el tiempo necesario; pero además se detalla mucho más cada una de estas obligaciones[166];
- los principios de seguridad[167] y confidencialidad[168] también se encuentran ampliamente desarrollados.

Con posterioridad a la Directiva 95/46/CE son muchas las sentencias del TJUE que se han pronunciado respecto al derecho fundamental a la protección de datos. En 2003 el TJCE lo hace en el caso *Österreichischer Rundfunk*[169], tras una cuestión

[165] Artículo 8.4 Directiva 95/46/CE: *"Toda autoridad de control entenderá de las solicitudes que cualquier persona, o cualquier asociación que la represente, le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Esa persona será informada del curso dado a su solicitud".*

[166] Artículo 6 Directiva 95/46/CE: *"Los Estados miembros dispondrán que los datos personales sean: a) tratados de manera leal y lícita; b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas; c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente; d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados; e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos".*

[167] Artículo 17 Directiva 95/46/CE: *"1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción , accidental o ilícita , la perdida accidental y contra la alteración, la difusión o el acceso no autorizado, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales".*

[168] Artículo 16 Directiva 95/46/CE: *"Las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, solo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal".*

[169] Caso *Rechnungshof* contra *Österreichischer Rundfunk*. STJCE de 20 de mayo de 2003, As. C-465/00, C-138/01 y C-139/01. Sobre el caso, PIÑAR MAÑAS, JL. "*El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas"*, en Cuadernos de Derecho Público, núm. 19-20, 2003, pp. 61-66.

prejudicial formulada por el *Verfassungsgerichtshof*[170]y el *Oberster Gerichtshof*[171] sobre la interpretación de la normativa nacional en relación con la Directiva por la que se obliga a un órgano estatal de control a recoger y comunicar, para su publicación, datos sobre los ingresos de personas empleadas por entidades que están sujetas a dicho control cuando tales ingresos superan un límite determinado[172].

En ese mismo año, la sentencia del caso *Lindqvist*[173] supuso la interpretación de la Directiva ante siete cuestiones prejudiciales formuladas por el *Göta hovrätt*[174] sueco en el marco de un proceso penal por incumplimiento de la legislación sueca de protección de datos[175]. Esta sentencia ha sido de especial relevancia por cuanto hay pronunciamientos expresos sobre el flujo de datos a través de internet. El TJCE estableció que la referencia de datos personales en una página web constituyen un *"tratamiento total o parcialmente automatizado de datos personales",* y que no estaba incluido en ninguna de las excepciones contenidas en la Directiva. Pero el punto clave de esta resolución es la consideración de que la difusión de datos personales en el contenido de una página web, de modo que sean accesibles a cualquiera que se conecte a internet, incluido quienes estén en terceros países, no constituye una transferencia de datos a un país tercero[176].

[170] Tribunal Constitucional Austriaco.

[171] Corte Suprema Austriaca

[172] El TJCE entiende que *"Del conjunto de las consideraciones precedentes resulta que procede responder a la primera cuestión que los artículos 6, apartado 1, letra c), y 7, letras c) y e), de la Directiva 95/46 no se oponen a una normativa nacional, como la controvertida en los asuntos principales, siempre que se demuestre que la amplia divulgación no sólo del importe de los ingresos anuales, cuando éstos superan un límite determinado, de las personas empleadas por las entidades sujetas al control del Rechnungshof, sino también de los nombres de los beneficiarios de dichos ingresos, es necesaria y apropiada para lograr el objetivo de buena gestión de los recursos públicos perseguido por el constituyente, extremo que ha de ser comprobado por los órganos jurisdiccionales remitentes".*

[173] STJCE de 6 de noviembre de 2003. Asunto C-101/01. Caso *Lindqvist*. Sobre el asunto tratado, LLANEZA GONZÁLEZ, P. *La protección de datos personales en el entorno web*. Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid, núm. 7, 2004.

[174] Tribunal de Apelación sueco.

[175] Estas cuestiones se suscitaron en el marco de un proceso penal seguido ante dicho órgano jurisdiccional contra la Sra. *Lindqvist,* acusada de haber infringido la normativa sueca relativa a la protección de datos personales al publicar en su sitio Internet diversos datos de carácter personal sobre varias personas que, como ella, colaboraban voluntariamente con una parroquia de la Iglesia protestante de Suecia.

[176] Para mayor estudio de la sentencia *Lindqvist,* PIÑAR MAÑAS, JL: *"El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas",* en Cuadernos de Derecho Público, núm. 19-20, 2003; PULIDO QUECEDO, M. *La*

El reconocimiento del derecho a la protección de datos como derecho fundamental en la Unión llegó en el año 2000, en Niza, cuando se proclamó la Carta de Derechos Fundamentales de la Unión Europea[177], si bien (como ya hemos expuesto anteriormente) no fue hasta su incorporación al Tratado de Lisboa[178] cuando adquirió fuerza vinculante y quedó incluido en el derecho originario de la Unión. Esta promulgación supuso la consolidación del derecho fundamental a la protección datos como un derecho independiente y autónomo, si bien no está exenta de críticas por su contenido insuficiente[179].

2.3.3 Legislación europea de protección de datos.

El derecho de la Unión Europea está formado por el denominado derecho primario (también llamado derecho originario) y por el derecho derivado. El primero, constituido por los Tratados, es el Derecho supremo de la Unión Europea que prevalece sobre cualquier otra fuente de derecho; y el segundo es el formado por reglamentos, directivas y decisiones adoptados por las distintas Instituciones de la

catequista y los riesgos de Internet, en AJA, núm. 602, 2003; y ROSSNAGEL, A. *EuGH: Personenbezogene Daten im Internet*, en Multimedia und Recht, 2/2004, p. 95-100.

[177] Consejo de Niza. 7 de diciembre de 2000. DOUE C 364, de 18 de diciembre.
Artículo 8 de la Carta: *"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".*

[178] DO C 306 de 17.12.2007.

[179] En este sentido RUIZ MIGUEL, C. *"El Derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea. Análisis crítico"*. Revista de Derecho Comunitario Europeo. Año 7, número 14. Enero-Abril 2003.
"La Carta, en lugar de «consolidar» esos cinco principios, supone un paso atrás en alguno de ellos. Tienen una recepción aceptable los principios de consentimiento y de calidad y lealtad que están recogidos de forma sucinta pero suficiente. No sucede lo mismo con los principios de información, de control y de seguridad y confidencialidad. El principio de información tal y como se recoge en la CDF sólo abarca el derecho a «demandar» información («derecho a acceder a los datos que le conciernan »), pero no parece que incluya el derecho a «recibir» información (es decir, deber del poseedor del responsable del fichero de comunicar al interesado los datos que obren en el mismo si antes no lo hubiera hecho ya). En cuanto al principio de control, el art. 8.2 CDF sólo alude a la posibilidad de «rectificación» de datos, pero omite la referencia a su borrado o cancelación. Por su parte, la CDF carece de cualquier alusión al principio de seguridad y de confidencialidad que ya estaba contemplado en el Convenio del Consejo de Europa de 1981".

Unión Europea, a las cuales se les ha otorgado dicha autoridad en virtud de los Tratados.

La normativa fundamental europea en materia de protección de datos, por orden cronológico, es la Directiva 95/46/CE del Parlamento y del Consejo, relativa a la protección de las personas físicas en los que respecta al tratamiento de datos personales y a la libre circulación de estos datos[180], que en breve será sustituida por el nuevo Reglamento General de Protección de Datos; la Carta de Derechos Fundamentales de la Unión Europea del año 2000[181] y el Reglamento (CE) 45/2001 del Parlamento Europeo y del Consejo sobre 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 sobre la libre circulación de estos datos[182]. Estas normas han dado lugar a otras, bien de desarrollo o bien de especialidad.

La Directiva 95/46/CE tiene ya veinte años de vida, muchos años para una normativa que regula la transferencia de datos en la era digital, en un sector tan cambiante y evolutivo como es la tecnología y donde los nuevos retos son constantes. Una nueva realidad que no existía hace veinte años, donde el flujo transfronterizo de datos ha cobrado unas dimensiones incalculables, donde las nuevas técnicas de recolección e intercambio de datos abren nuevos campos, el *big data*, el *cloud computing*…. Ante esta situación, la Comisión Europea tras numerosos trabajos y consultas propuso un nuevo marco jurídico, un Reglamento General de Protección de Datos que armonizase las distintas legislaciones nacionales, sustituyera a la actual Directiva y se adaptara a la nueva realidad.

Así pues, la norma que esperemos se adecue a nuestros tiempos y necesidades, y que está pendiente de aprobación en un breve espacio de tiempo es el nuevo Reglamento de Protección de Datos de la Unión Europea, que a fecha de hoy se encuentra en

[180] Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en los que respecta al tratamiento de datos personales y a la libre circulación de estos datos. L 281, de 23 de noviembre de 1995.

[181] Consejo de Niza. 7 de diciembre de 2000. DOUE C 364, de 18 de diciembre.

[182] Reglamento (CE) 45/2001 del Parlamento Europeo y del Consejo de 18 de diciembre de 2000 sobre 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 sobre la libre circulación de estos datos. DO 2001 L 8.

proceso de discusión a tres bandas, el famoso trílogo, donde tanto la Comisión como el Parlamento y el Consejo han presentado sus propuestas y está pendiente de acordarse un documento final.

2.3.3.1 Directiva 95/46/CE[183] del Parlamento y del Consejo.

La Directiva 95/46/CE es el texto de referencia en materia de protección de datos a nivel europeo, es el principal instrumento jurídico. Cuando se dictó en el año 1995 no existía el reconocimiento de la protección de datos como tal en la Comunidad, por lo que no había competencias para legislar sobre una temática que no formaba parte de las políticas de la Unión, no estaba reconocida como derecho fundamental y tampoco aparecía en los Tratados constitutivos. Pero la visión de la importancia de la regulación del tratamiento de datos personales estaba constatada y de hecho se creó una Unidad de Protección de Datos, si bien inicialmente formaba parte de la Dirección General de Mercado Interior (por ello el nombre de la Directiva habla de "circulación de datos", para que de este modo tuviera encaje en el derecho de la Unión). Posteriormente, en el año 2004 se trasladó a la Dirección General de Justicia, siendo el Jefe de Unidad en aquel momento *Philippe Renaudière*, actual *Data Protection Officer* (DPO) de la Comisión Europea[184].

La Directiva surge en el ánimo de la aproximación de las normas nacionales europeas que ya existían con anterioridad a ella, además de dotar de mayor contenido este derecho del que ya se le había otorgado en el Convenio 108 del Consejo de Europa, pues todos los países que en ese momento eran miembros de la Comunidad también eran firmantes de dicho instrumento. Crea un marco regulador armonizado para todos los países de la Unión estableciendo un equilibrio entre la protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea. Con dicha aproximación se pretendían eliminar las contradicciones entre las disposiciones legislativas y administrativas de los Estados miembros o

[183] DO L 281 de 23.11.1995, p. 31/50.

[184] Conversaciones con LEONARDO CERVERA NAVAS, *Head of Human Resources and Administration* en el Supervisor Europeo de Protección de Datos. Bruselas 15 de septiembre de 2015.

suprimir paso a paso las diferencias, con el fin de que en todos los Estados miembros se impusieran en lo posible los mismos requisitos materiales[185]. El ámbito territorial de la Directiva de protección de datos es de aplicación además de a los 28 Estados miembros de la Unión Europea, a los Estados no miembros de la UE que forman parte del Espacio Económico Europeo[186] (EEE), tales como Islandia, Liechtenstein y Noruega.

Pero, tal y como reconoció el TJUE[187], la armonización de estas normas no es una armonización mínima, sino completa, señalando con ello el poco margen que se le dejaba a la normativa nacional de trasposición, cuestión no del todo compartida a fecha de hoy por cuanto los agentes económicos se quejan del obstáculo que supone para el desarrollo económico y comercial la existencia de regulación distinta en los diferentes países de la Unión Europea, especialmente en materias como el flujo transfronterizo de datos, siendo ésta una de las cuestiones claves para el impulso del nuevo texto que está en proceso de aprobación; y ello porque si bien la Directiva como instrumento marco expone los objetivos a conseguir, son los Estados miembros en la transposición a su normativa quienes deciden cómo regular para conseguir dichos objetivos. En ocasiones, esa transposición puede ser mínima o no darse, con el consecuente perjuicio para los ciudadanos que tienen derecho a invocar su efecto directo ante las autoridades de su país.

A diferencia de otras normas anteriores, la Directiva 95/46 es de aplicación a todos los datos de carácter personal, automatizados o no automatizados, siempre que estos últimos estén contenidos o destinados a ser incluidos en un fichero; y ello con determinadas excepciones tales como el uso de esos datos en el ejercicio de actividades particulares o domésticas o materias reservadas a la soberanía de cada

[185] El ABC del Derecho de la Unión Europea. DR. KLAUS-DIETER BORCHARDT. Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2011.
Disponible en:
http://bookshop.europa.eu/es/el-abc-del-derecho-de-la-uni-n-europea-pbOA8107147/.

[186] Acuerdo sobre el Espacio Económico Europeo, DO 1994 L 1, el cual entró en vigor el 1 de enero de 1994.

[187] TJUE, asuntos acumulados C-468/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) contra Administración del Estado, de 24 de noviembre de 2011, apartados 28-29.

país en las que no se aplica el derecho comunitario, como la seguridad pública, la defensa o la seguridad del Estado[188].

El objeto de la Directiva 95/46 es *"la protección de las libertades y los derechos fundamentales de las personas físicas y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales"* (art. 1). Para cumplirlo establece los principios que determinarán la licitud del tratamiento de datos, y que ya formaban parte del Convenio 108 del Consejo de Europa, si bien los dota de mayor contenido: la calidad de los datos (art. 6), la legitimación del tratamiento (art. 7), las categorías especiales del mismo (art. 8), la información a los afectados (art. 10), el derecho de acceso del interesado a los datos (art. 12), las excepciones y limitaciones a esos principios, tales como la seguridad del Estado, la defensa, la seguridad pública, la represión de infracciones penales (art. 13), el derecho de oposición al tratamiento por el interesado (art. 14), la confidencialidad y la seguridad del tratamiento (art. 16) o la notificación del mismo a la Autoridad de Control (art. 18), la obligación de los Estados miembros de disponer de un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables al tratamiento de que se trate (art. 22), así como la autorización de la realización de transferencias de datos personales de un Estado miembro a un tercer país siempre y cuando se garantice un nivel de protección adecuado (art. 25).

[188] Considerando (13) de la Directiva 95/46/CE: *"Considerando que las actividades a que se refieren los títulos V y VI del Tratado de la Unión Europea relativos a la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en el ámbito penal no están comprendidas en el ámbito de aplicación del Derecho comunitario, sin perjuicio de las obligaciones que incumben a los Estados miembros con arreglo al apartado 2 del artículo 56 y a los artículos 57 y 100 A del Tratado; del] tratamiento de los datos de carácter personal que sea necesario para la salvaguardia del bienestar económico del Estado no está comprendido en el ámbito de aplicación de la presente Directiva en los casos en que dicho tratamiento esté relacionado con la seguridad del Estado".*
Artículo 3.2 Directiva 95/46/CE: *"2. 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 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;
- efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas".

Dos hitos en materia de organismos nacen de la Directiva: la obligatoriedad de Autoridades públicas de control en todos los países miembros (artículo 28); y la creación de un Grupo de Trabajo en materia de protección de datos de carácter consultivo (artículo 29), el que será denominado Grupo Europeo de Protección de Datos del artículo 29 o GT29, formado por los representantes de las Autoridades de control nacionales, por representantes de las Autoridades de control de las instituciones y organismos comunitarios y por un representante de la Comisión.

En cuanto a las Autoridades de control nacionales, prevé la Directiva que sus competencias serán las siguientes:

- Vigilancia de la aplicación de la normativa de desarrollo de la Directiva 95/46/CE.
- Obligación de consulta por parte del órgano legislativo nacional en la elaboración de las medidas reglamentarias o administrativas relativas a la protección de datos.
- Poder de investigación como el derecho de acceso para recabar la información necesaria en el desarrollo de su misión de control.
- Poderes de intervención, tales como formular dictámenes antes de realizar determinados tratamientos, garantizar la publicación de los mismos, ordenar el bloqueo, supresión o destrucción de datos, prohibir provisional o definitivamente un tratamiento, dirigir una advertencia o amonestación al responsable del tratamiento o someter la cuestión a los parlamentos u otras instituciones políticas nacionales.
- Capacidad procesal en caso de infracciones de las disposiciones nacionales adoptadas en aplicación de la Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial.

En relación a estas funciones, establece el apartado 6 del artículo 28 que toda autoridad de control será competente para ejercer en el territorio de su propio Estado miembro los poderes que acabamos de describir. Es importante resaltar este punto que ha sido recientemente analizado e interpretado en la sentencia del Tribunal de

Justicia de la Unión Europea de 6 de octubre de 2015, caso *Maximillian Schrems* vs Facebook, la cual desglosamos en el apartado 3.4.2.

La Jurisprudencia del TJUE interpretando la Directiva 95/46/CE ha sido muy numerosa dadas las diferencias o contradicciones que en algunos casos presentaba con respecto a la normativa nacional de desarrollo.[189] La sentencia de 20 de mayo de 2003, *Österreichischer Rundfunk*, determinó por ejemplo que *"ninguna razón de principio permite excluir a las actividades profesionales… del concepto de vida privada",* con lo que incluía en el derecho fundamental a la protección de datos determinados datos de la vida profesional que para algunas legislaciones queda fuera del su ámbito de protección[190]. Se hace referencia además en esta sentencia a la invocación por parte de los particulares de la aplicación directa de la Directiva. La sentencia *Lindqvist*[191] de 6 de noviembre de 2003 también aclaró que el tratamiento de datos personales por particulares en internet supone un tratamiento de datos, tal y como establece la Directiva, en toda regla.

Jurisprudencia más reciente encontramos en la STJUE de 11 de diciembre de 2014[192], donde el Tribunal de la República Checa (*el Nejvyšší správní soud*) formula petición de decisión prejudicial a fin de que el TJUE se pronuncie acerca de la interpretación del artículo 3.2 de la Directiva en cuanto a si la grabación de imágenes *"debe interpretarse en el sentido de que la utilización de un sistema de cámara de*

[189] STJCE de 14 de octubre de 1999. Caso Adidas, Conclusiones del Abogado General *Cosmas* de 10.06.1999, donde analiza el derecho de acceso a los datos personales, subrayando la necesidad de ponderar intereses contrapuestos y no entender el derecho a la protección de datos como absoluto.
En relación al caso Adidas, JL.PIÑAR MAÑAS, *El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas*. Cuadernos de Derecho Público, números 19-20, 2003, p. 66-68.
STJCE de 14 de octubre de 2000. Caso *The Queen and the Ministry of Agriculture, Fischeries and Food*. Conclusiones presentadas por el Abogado General *Alber* el 10 de febrero de 2000, en cuanto al carácter exacto y completo del derecho de información en el tratamiento de datos personales.

[190] Es el caso de la normativa española, donde para la Ley Orgánica 15/99 (LOPD), los datos profesionales no se consideran datos de carácter personal. El propio Tribunal Constitucional ha sido vacilante en su jurisprudencia, dictando sentencias donde expresamente dice que los datos sociales y profesionales en que el trabajador desempeña su actividad no se integran, en principio, en la esfera privada de la persona (SSTC 180/1987, de 12 de noviembre; 142/1993, de 22 de abril o 202/1999 de 8 de noviembre) y otras sentencias en las que del conjunto de hechos relativos a las relaciones profesionales puede resultar posible acceder a informaciones sobre la vida personal del trabajador (SSTC 142/93).

[191] Ver 175.

[192] Asunto C-212/13. *František Ryneš y Úřad pro ochranu osobních údajů* (Agencia de Protección de Datos Checa).

vídeo, que da lugar a la obtención de imágenes de personas que luego se almacenan en un dispositivo de grabación continuada, como un disco duro, sistema de videovigilancia instalado por una persona física en su vivienda familiar con el fin de proteger los bienes, la salud y la vida de los propietarios de la vivienda y cuya vigilancia cubre asimismo el espacio público, constituye un tratamiento de datos efectuado en el ejercicio de actividades exclusivamente personales o domésticas a efectos de la citada disposición", concluyendo finalmente el Tribunal que dicha actuación *"no constituye un tratamiento de datos efectuado en el ejercicio de actividades exclusivamente personales o domésticas a efectos de la citada disposición de la Directiva".*

Relevancia especial merece la sentencia del TJUE de 13/05/2014[193], conocida como la "sentencia del derecho al olvido", en resolución de cuestión prejudicial planteada por la Audiencia Nacional de España en el procedimiento de *Google Spain*, S.L. y *Google Inc*. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González. El procedimiento del que trae causa en España es una denuncia formulada ante la AEPD por el sr. Costeja por la que se estimó la reclamación de este último contra *Google Spain*, S.L. y *Google Inc*. y se ordenaba a *Google Inc*. que adoptara las medidas necesarias para retirar los datos personales del Sr. Costeja González de su índice e imposibilitara el acceso futuro a los mismos.

El inicio del procedimiento tiene su origen en la denuncia presentada por el sr. Costeja ante la AEPD contra un periódico nacional[194] y contra *Google Inc*, ya que cuando se introducían los datos del reclamante en el motor de búsqueda de Google aparecían vínculos hacia páginas del citado diario en las que figuraba un anuncio de una subasta de inmuebles vinculada a unas deudas con la Seguridad Social, siendo que este problema ya había desaparecido y no existía en el momento de la reclamación dicha deuda.

El sr. Costeja solicitaba dos cosas: por un lado que el periódico eliminara o modificara la publicación para que no apareciesen sus datos personales, o bien utilizara las herramientas facilitadas por los motores de búsqueda para proteger esos

[193] Sentencia del TJUE 13.05. 2014 (Gran Sala). Asunto C-131/12. Google vs AEPD y Mario Costeja.
[194] La Vanguardia Ediciones SL

datos; y por otro lado que exigiese a *Google Spain* o a *Google Inc.* que eliminaran u ocultaran sus datos personales para que dejaran de aparecer en la búsqueda ligados a la publicación del diario.

La AEPD desestimó la petición respecto del periódico, pues dicha publicación estaba legalmente justificada, y la estimó respecto de *Google Spain* y *Google Inc*. La AEPD consideró que quienes gestionaban motores de búsqueda estaban sometidos a la normativa de protección de datos y que lo que hacían suponía un tratamiento de datos, considerándose autorizada para ordenar la retirada e imposibilitar el acceso a determinados datos por parte de los motores de búsqueda. *Google Spain* y *Google Inc*. interpusieron dos recursos ante la Audiencia Nacional, que ésta decidió acumular.

Para la Audiencia Nacional la cuestión era determinar las obligaciones en materia de protección de datos de los motores de búsqueda sobre las personas que no quieren que sus datos aparezcan indexados en webs de terceros. Para ello elevó al TJUE tres cuestiones prejudiciales, una relacionada con la interpretación de establecimiento del artículo 4.1.a de la Directiva; otra sobre si la actividad del motor de búsqueda se podía considerar un tratamiento de datos y, en su caso, responsable del tratamiento, y por ende requerirle al buscador la retirada de los índices (todo ello en interpretación de los artículos 2.b, 2.d, 12.b y 14.a de la Directiva); y por último también respecto del artículo 12.b y 14.a, si los derechos de supresión, bloqueo y oposición comprenden que el interesado pueda dirigirse a los buscadores para impedir la indexación cuando considere que esa información pueda perjudicarle o desee que sea olvidada aunque sea una información publicada lícitamente por terceros.

La sentencia que analizamos era esperada "como agua de mayo" por la comunidad internauta, y fueron muchos los litros de tinta que se vertieron tanto antes de ser conocida como después.

El 13 de mayo de 2014 el TJUE dictó sentencia en la que, con base en la Directiva 95/46/CE, reconocía que la actividad del motor de búsqueda debe calificarse de tratamiento de datos personales y el gestor deberá considerarse responsable de dicho tratamiento; que existía un establecimiento del responsable en territorio de Estado

miembro[195]; que el gestor del motor de búsqueda está obligado a eliminar de la lista de resultados obtenida a partir del nombre de una persona vínculos a webs de terceros aunque éstos no lo borren previamente y aunque sea lícita[196]; y que este "derecho de borrado" puede no existir en situaciones muy concretas cuando el interesado sea una persona pública, debiendo de proceder a una ponderación del derecho fundamental a la protección de datos y el derecho a la información, pudiendo predominar este último[197].

De este modo, cualquier ciudadano tiene derecho a que se eliminen del motor de búsqueda de Google datos personales que no quiera que aparezcan, siempre y cuando estén desactualizados y no tengan relevancia pública. Tras las numerosísimas reclamaciones interpuestas ante la AEPD posteriores a la sentencia solicitando de Google retirar la indexación de determinados datos personales, la compañía se acoge casi siempre en sus alegaciones a la relevancia pública del asunto, debiendo ser la Autoridad de control quien tenga que proceder en esta instancia a la ponderación de los derechos fundamentales reclamados.

Esta importantísima sentencia trajo consigo un documento del GT29[198]sobre aplicación de la misma, desarrollando los criterios interpretativos comunes para aplicar la sentencia por parte de las Autoridades de control de los Estados miembros[199].

[195] Ver 193. Sentencia del TJUE 13 de mayo de 2014, apartado 20: *"Cuando el gestor de un motor de búsqueda crea en el estado miembro una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro".*

[196] Ver 193. Sentencia del TJUE 13 de mayo de 2014, apartado 62: *"El gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita".*

[197] Ver 193. Sentencia del TJUE 13 de mayo de 2014, punto 4 del fallo: *"El interesado… puede… solicitar que la información ya no se ponga a disposición del público en general… sin embargo, tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate".*

[198] Grupo de Trabajo del Artículo 29.

[199] Documento del GT 29 para la aplicación de criterios uniformes sobre el "derecho al olvido", de 27.11.2014:

También el nuevo Reglamento General de Protección de Datos prevé este derecho en su artículo 17[200].

La más novedosa y esperada sentencia interpretativa de la Directiva 95/46/CE es la STJUE de 6 de octubre de 2015 (a la que ya hemos hecho referencia) en el caso *Schrems* contra Facebook[201], C-362/14, donde el Tribunal ha profundizado en la interpretación de los artículos 25 y 28 de la citada Directiva en relación con la Decisión de la Comisión 2000/520, acuerdo de Puerto Seguro. La cuestión prejudicial de fondo es si dicho artículo 25 apartado 6, en relación a los artículos 7, 8 y 47 de la Carta de Derechos Fundamentales debe interpretarse en el sentido de que una decisión, como la Decisión 2000/520, por la que la Comisión constata que un tercer país garantiza un nivel de protección adecuado, impide que una Autoridad de control de un Estado miembro, a la que se refiere el artículo 28 de la Directiva, pueda examinar la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen, que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona afirma que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado[202]. Entiende el Tribunal que la Directiva ha de ser interpretada siempre a la luz de los derechos fundamentales recogidos en la Carta y que el artículo 28 se aplica por su propia naturaleza a todo tratamiento de datos personales, por lo que incluso habiendo adoptado la Comisión una decisión en virtud del artículo 25, apartado 6, de esa Directiva, las Autoridades nacionales de control, a las que una persona haya presentado una solicitud de protección de sus derechos y libertades

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2014/notas_prensa/common/nov_14/wp225_en.pdf.

[200] Artículo 17 Reglamento General de Protección de Datos, texto de la Comisión: *"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".*

[201] Ver 42.

[202] Sentencia TJUE asunto C‑362/14. *Schrems vs Facebook*. Apartado 37.

frente al tratamiento de datos personales que la conciernen, deben poder apreciar con toda independencia si la transferencia de esos datos cumple las exigencias establecidas por la referida Directiva.

Las consecuencias de dicha interpretación no eran minúsculas, pues con ella temblaban las bases del sistema comercial entre Europa y Estados Unidos, pudiendo cualquier Autoridad de control nacional de Protección de Datos de la Unión Europea ordenar el cese de la transferencia de datos personales a los Estados Unidos de América. Dicha sentencia ha declarado nulo el Acuerdo *Safe Harbour*[203] con las consecuencias que detallamos en el apartado 3.4.2.3.

2.3.3.2 Otras Directivas del Parlamento y del Consejo de interés.

A partir de la entrada en vigor de la Directiva 95/46/CE, son muchas otras las que se han publicado en materia de protección de datos para tratar temas más específicos que requieren de aclaración y ponderación con otros intereses legítimos.

A.- Sobre la privacidad en las comunicaciones.

En esta materia ya se legisló en el ámbito de la Comunidad en 1997 con la Directiva 97/66/CE[204] relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, la cual fue derogada posteriormente por la Directiva 2002/58/CE[205], sobre la privacidad y las comunicaciones

[203] Decisión 2000/520/CE: Decisión de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América [notificada con el número C(2000) 2441] (Texto pertinente a efectos del EEE.)
DO L 215 de 25.8.2000, p. 7/47.

[204] Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. DO L 24 de 30.1.1998, p. 1-8.

[205] 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. DO L 201 de 31.7.2002, p. 37-47.
Esta Directiva se adoptó al mismo tiempo que un nuevo grupo de normas destinadas a servir de marco al sector de las comunicaciones electrónicas, en las que se incluyen disposiciones sobre

electrónicas, modificada a su vez esta última en parte por la Directiva 2006/24/CE[206] sobre conservación de datos, así como por la Directiva 2009/136/CE[207], que modificaba varias Directivas y el Reglamento (CE) 2006/2004[208].

La Sentencia del TJUE de 8 de abril de 2014[209] declaró inválida la Directiva sobre conservación de datos, y ello porque consideraba que constituye una injerencia de gran magnitud y especial gravedad en los derechos al respeto de la vida privada y de la protección de datos de carácter personal.

temas tales como la conservación de los datos de conexión por parte de los Estados miembros a efectos de vigilancia policial (retención de datos), el envío de mensajes electrónicos no solicitados, la utilización de los denominados "chivatos"(*cookies*) y la inclusión de datos personales en las guías públicas.

[206] Directiva 2006/24/CE206, 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. DO L 105 de 13.4.2006, p. 54-63.
Al respecto, LÓPEZ-BARAJAS PEREA, M.I. *El deber de conservación de datos en la Unión Europea y sus límites.* Revista de derecho de la Unión Europea, núm. 16, 2009, p. 195-220.

[207] Directiva 2009/136/CE[207] 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) 2006/2004 sobre la cooperación entre las autoridades nacionales encargadas de la aplicación de la legislación de protección de los consumidores.
DO L 337 de 18.12.2009, p. 11-36.

[208] Reglamento (CE) 2006/2004. DO L 364 de 9.12.2004, p. 1-11.

[209] Sentencia del TJUE (Gran Sala) de 8 de abril de 2014. Cuestiones prejudiciales presentadas por la *High Court* (Tribunal Superior de Irlanda) y el *Verfassungsgerichtshof* (Tribunal Constitucional de Austria) Asuntos acumulados C-293/12 y C-594/12. *Digital Rights Ireland Ltd* contra *Minister for Communications, Marine and Natural Resources* y otros; y *Kärntner Landesregierung* y otros.
"El Tribunal de Justicia considera que, al imponer la conservación de estos datos y al permitir el acceso a las autoridades nacionales competentes, la Directiva se inmiscuye de manera especialmente grave en los derechos fundamentales al respeto de la vida privada y a la protección de datos de carácter personal. ...Considera que el legislador de la Unión sobrepasó los límites que exige el respeto del principio de proporcionalidad, y ello por las siguientes razones: ...abarca de manera generalizada a todas las personas, medios de comunicación electrónica y datos relativos al tráfico sin que se establezca ninguna diferenciación, limitación o excepción en función del objetivo de lucha contra los delitos graves; ...no fija ningún criterio objetivo que permita garantizar que las autoridades nacionales competentes únicamente tendrán acceso a los datos y podrán utilizarlos para prevenir, detectar o reprimir penalmente delitos que, por la magnitud y la gravedad de la injerencia en los derechos fundamentales en cuestión, puedan considerarse suficientemente graves para justificar tal injerencia;... y por último en lo que atañe al período de conservación de los datos, la Directiva prescribe un período mínimo de seis meses sin establecer ninguna distinción entre las categorías de datos en función de las personas afectadas o de la posible utilidad de los datos con respecto al objetivo perseguido". Comunicado de Prensa núm. 54/14 del TJUE, hecho en Luxemburgo el 8 de abril de 2014.

B.- Sobre la firma electrónica.

En el ánimo de potenciar la confianza y seguridad de las comunicaciones electrónicas, en 1999 se dicta la Directiva 1999/93/CE[210], del Parlamento Europeo y del Consejo, por la que se establece un marco comunitario para la firma electrónica; Directiva que ha sido derogada por el Reglamento 910/2014[211] del Parlamento Europeo y del Consejo relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Esta Directiva trajo consigo la seguridad jurídica con respecto a la admisibilidad general de la firma electrónica.

C- Sobre el acceso a redes y a las comunicaciones.

Han sido varias las normas que se han desarrollado al respecto, tales como la Directiva 2002/19/CE[212], del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva de acceso); la Directiva 2002/20/CE[213], del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva de autorización); o la Directiva 2002/22/CE[214] 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 servicio universal),

[210] Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999. DO L 13 de 19.1.2000, p. 12-20.

[211] Reglamento 910/2014 del Parlamento Europeo y del Consejo 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga. DO L 257 de 28.08.2014, p. 73-114.

[212] Directiva 2002/19/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva de acceso). DO L 108 de 24.4.2002, p. 7-20.

[213] Directiva 2002/20/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva de autorización). DO L 108 de 24.4.2002, p. 21-32.

[214] 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 servicio universal). DO L 108 de 24.4.2002, p. 51-77.

modificada por la Directiva 2009/136/CE[215] del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009.

El TJUE se ha pronunciado en varias ocasiones acerca de la interpretación de estas Directivas. En España fue llamativo el caso presentado por Vodafone en la jurisdicción ordinaria española en la que reclamaba la no procedencia del pago de un canon municipal por instalación de recursos cuando no era propietaria de los mismos, sino que simplemente los utilizaban para prestar los servicios. El Tribunal Supremo interrogó al TJUE para que se pronunciase sobre la interpretación del artículo 13 de la Directiva de autorización, dictaminando la sentencia[216] que dicho artículo *"debe interpretarse en el sentido de que se opone a la aplicación de un canon por derechos de instalación de recursos en una propiedad pública o privada, o por encima o por debajo de la misma, a los operadores que, sin ser propietarios de dichos recursos, los utilizan para prestar servicios de telefonía móvil".*

D.- Sobre el comercio electrónico.

En el año 2000 se dictó La Directiva 2000/31/CE[217], del Parlamento Europeo y del Consejo, sobre el comercio electrónico.

[215] 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.
DO L 337 de 18.12.2009, p. 11-36.

[216] Sentencia del TJUE (Sala cuarta) de 12 de julio de 2012. Asuntos acumulados C-55/11, C-57/11 y C-58/11, en procedimientos entre Vodafone España SA y Ayuntamiento de Santa Amalia; Vodafone España SA y Ayuntamiento de Tudela; y entre France Telecom España SA y Ayuntamiento de Torremayor, respectivamente. En esencia, *"Se desprende de las resoluciones de remisión que, al amparo de la normativa española, varios municipios del Reino de España, entre ellos los Ayuntamientos de Santa Amalia, Tudela y Torremayor, aprobaron ordenanzas fiscales que gravan a las empresas con cánones por el uso privativo o el aprovechamiento especial del dominio público municipal hecho con el fin de prestar servicios de suministro de interés general, tanto si dichas empresas son propietarias de las instalaciones necesarias para prestar tales servicios y que ocupan materialmente ese dominio, como si no lo son. La prestación de servicios de telefonía móvil figura entre los servicios gravados en aplicación de dichas ordenanzas".*

[217] Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior. DO L 178 de 17.7.2000, p. 1-16.

También en este asunto la jurisprudencia comunitaria ha tenido que pronunciarse en varias ocasiones. En el año 2006 el Juzgado de lo Mercantil núm. 5 de Madrid, en el caso Promusicae vs Telefónica[218], planteó ante el TJUE una cuestión prejudicial acerca de si debe interpretarse esta Directiva (en relación a otras normas en materia de propiedad intelectual) en el sentido de que obligue a los Estados miembros a imponer el deber de comunicar datos personales en el marco de un procedimiento civil con objeto de garantizar una protección efectiva de los derechos de autor. El TJUE sentenció en sentido negativo, entendiendo que no existe esa obligación. Esta sentencia tuvo mucha repercusión, pues además el TJUE recordó la obligación de los Estados miembros de adaptar a su ordenamiento jurídico interno estas Directivas basándose en una interpretación que garantice un justo equilibrio entre los distintos derechos fundamentales protegidos por el ordenamiento jurídico comunitario.

E.- Sobre datos de transporte.

Se hizo necesario regular los datos personales de las personas que se transportaban, y ello a través de la Directiva 2004/82/CE[219], del Consejo de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas.

Los datos a los que se refiere la Directiva son los datos del sistema API[220] (distintos de los datos PNR), que recolecta los datos de los pasajeros por adelantado con la finalidad principal del control de identidad en los pasos fronterizos europeos y en el combate a la inmigración ilegal, para lo que se comunican anticipadamente los datos

[218] Sentencia del TJUE de 29 de enero de 2008. Asunto C-275/06. En el procedimiento del que trae causa la cuestión, Promusicae (Asociación de Productores de Música de España) solicitó al Juzgado que se ordenase a Telefónica revelar la identidad y dirección de determinadas personas a las que esta última presta un servicio de acceso a Internet y de las que se conoce su dirección «IP», así como la fecha y hora de conexión pues utilizaban un programa P2P que permitía el acceso, en una carpeta compartida de su ordenador personal, a fonogramas cuyos derechos patrimoniales de explotación corresponden a los asociados de Promusicae.

[219] 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. DO L 261 de 6.8.2004, p. 24/27.

[220] *Advance Passenger Information*, Información anticipada de los pasajeros.

de las personas transportadas por parte de los transportistas a las autoridades competentes en cada Estado europeo[221].

Todas estas directivas suponen nuevos actos legislativos que ayudarán a conformar la jurisprudencia posterior del TJCE en materia de protección de datos.

2.3.3.3 El Reglamento (CE) nº 45/2001, del Parlamento Europeo y del Consejo.[222]

El Reglamento 45/2001/CE surge en desarrollo del mandato que el legislador da al modificar a través del Tratado de Amsterdam[223] el artículo 286 del Tratado Constitutivo de la Unión Europea (TCE)[224], llevando al derecho originario la

[221] No debemos confundir los datos API con los datos PNR (*Passenger Name Records*), los cuales se utilizan principalmente como un instrumento para la prevención y represión de ilícitos terroristas y formas graves de delitos transnacionales.
El PNR es un fichero centralizado que contiene la información que las compañías aéreas recaban de sus pasajeros y que incluyen datos personales con muchísima información capaz de hacer un perfil del individuo. La Comisión, mediante la Decisión 2004/535/CE, consideró que la CBP (Servicio de Aduanas y Protección de fronteras de los EEUU) 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, y el 28/05/2004 se firmó el 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 DO L 142M), en el que se podían transferir hasta 34 elementos. Esta Decisión fue criticada tanto por el Supervisor Europeo de Protección de Datos como por el GT29. El 30 de mayo de 2006, el TJUE dictó sentencia por la que anulaba ambas Decisiones. Mediante la Decisión 2007/551/PESC/JAI del Consejo, de 23 de julio de 2007 (DO L 204), el Consejo aprobó otro acuerdo. A raíz de la entrada en vigor del Tratado de Lisboa, en 2011 se firmó un nuevo Acuerdo PNR con EEUU que entró en vigor el 1 de julio de 2012. En febrero de 2011 se presentó una propuesta de Directiva relativa a la utilización de datos de pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves, que supondría la instauración de un sistema PNR que afectaría a los vuelos entre la UE y países terceros y obligaría a las aerolíneas a comunicar a las autoridades nacionales del Estado miembro de origen o de destino los datos de los pasajeros. Dicha propuesta fue rechazada en abril de 2013 por la Comisión de Libertades Civiles, Justicia y Asuntos de Interior por entender que se vulneraba el derecho a la protección de datos de carácter personal. La propuesta se bloqueó en el Parlamento y actualmente, tras los atentados de *Charlie Hebdo* en París se ha intentado desbloquear y se encuentra en primera lectura.

[222] DO L 8 de 12.1.2001, p. 1-22.

[223] Tratado de Amsterdam por el que se modifican el Tratado de la Unión Europea, los Tratados Constitutivos de las Comunidades Europeas y determinados actos conexos, de 2 de octubre de 1997.
DO C 340 de 10.11.1997.

[224] Artículo 286 TCE: "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

necesidad de que el tratamiento de datos personales en el ámbito comunitario respondiera de igual modo a los estándares de la Directiva 95/46/CE.

Si bien la Directiva 95/46/CE tiene como objeto dotar de un marco jurídico armonizado en materia de protección de datos a los distintos Estados miembros de la Unión Europea, el Reglamento (CE) nº 45/2001 crea el marco normativo que garantiza un alto nivel de protección de los datos personales gestionados por las instituciones y organismos comunitarios: "*Las instituciones y los organismos creados por los Tratados constitutivos de las Comunidades Europeas o en virtud de dichos Tratados, en lo sucesivo denominados "instituciones y organismos comunitarios", garantizarán, de conformidad con el presente Reglamento, la protección 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 no limitarán ni prohibirán la libre circulación de datos personales entre ellos o entre ellos y destinatarios sujetos al Derecho nacional de los Estados miembros adoptado en aplicación de la Directiva 95/46/CE"* (art. 1). Y ello, *…"en la medida en que dicho tratamiento se lleve a cabo para el ejercicio de actividades que pertenecen al ámbito de aplicación del Derecho comunitario"* (art.3).

El Reglamento contiene un articulado con mucho paralelismo al de la Directiva: establece el principio de calidad de los datos, para lo que exige que éstos (automatizados o no) deberán ser tratados de manera leal y lícita, recogidos con fines determinados, explícitos y legítimos, y no tratarse posteriormente de manera incompatible con dichos fines. Serán también los datos los adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten después; así como exactos y, cuando sea necesario, actualizados; conservándose en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos o para los que se

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".

traten posteriormente (art. 4). Asimismo, establece criterios de legitimidad del tratamiento (artículos 5 a 9); categorías especiales de tratamientos (art. 10); información al interesado (art. 11); derechos de los interesados (artículos 13 a 19); confidencialidad (art. 21) o seguridad (art. 22).

Crea por vez primera la figura del Responsable de la protección de datos (art. 24) para cada institución u organismo comunitario[225], cuya función consiste en cooperar con el Supervisor en la protección de datos y velar porque el tratamiento no afecte negativamente a los derechos y libertades de las personas afectadas, por lo que su misión es doble: preventiva a la vez que proactiva. Es el punto de encuentro entre el responsable del tratamiento, el titular de los datos y la Autoridad de control.

La regulación del Responsable de Protección de Datos (DPO -*Data Protection Officer*- o Delegado de Protección de Datos) en el nuevo Reglamento General de Protección de Datos es uno de los temas polémicos cuyo alcance está por determinar y que ha suscitado numerosas opiniones encontradas. Si comparamos esta figura con el responsable de seguridad que establece el Real Decreto 1720/2007[226], por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de protección de datos española, podemos apreciar gran similitud, si bien el Responsable de Seguridad en España, tal y como actualmente está configurado, tiene menos competencias y menos independencia (por no decir ninguna) que el Responsable de la Privacidad que crea el futuro Reglamento.

Importantísima es en este Reglamento (CE) 45/2001, a los efectos del estudio que aquí realizamos, la creación en el artículo 41 de una Autoridad de control independiente como es el Supervisor Europeo de Protección de Datos, en cuyo detalle profundizaremos más adelante: *"1. Se instituye una autoridad de control independiente denominada «Supervisor Europeo de Protección de Datos». 2. Por lo que respecta al tratamiento de los datos personales, el Supervisor Europeo de*

[225] El *Data Protection Officer* (DPO) también es conocido como *Corporate Privacy Officer* (CPO), *Chief Privacy Officers* (CPO), *Correspondant Informatique et Libertés* (CIL), Oficial de Privacidad o Responsable de Privacidad.

[226] Artículos 95 y 109 del 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.

Protección de Datos velará porque los derechos y libertades fundamentales de las personas físicas, en particular el derecho de las mismas a la intimidad, sean respetados por las instituciones y los organismos comunitarios. El Supervisor Europeo de Protección de Datos garantizará y supervisará la aplicación de las disposiciones del presente Reglamento y de cualquier otro acto comunitario relacionado con la protección de los derechos y libertades fundamentales de las personas físicas en lo que respecta al tratamiento de datos personales por parte de una institución u organismo comunitario, y asesorará a las instituciones y a los organismos comunitarios, así como a los interesados, en todas las cuestiones relacionadas con el tratamiento de datos personales. Con este fin ejercerá las funciones establecidas en el artículo 46 y las competencias que le confiere el artículo 47".

También en interpretación de este Reglamento se ha tenido que pronunciar el TJUE en varias ocasiones. Así, en la sentencia del TJUE de 29 de junio de 2010[227], asunto Comisión vs *Bavarian Lager*, el Tribunal de Justicia precisa el alcance de la protección de los datos personales en el marco del acceso a los documentos de las instituciones de la Unión. Entiende el Tribunal que si no hay justificación expresa y legítima que acredite la necesidad de revelar datos personales en el acceso a un documento público ni se puede verificar que no existían motivos para suponer que una transmisión no perjudicaría los intereses legítimos de los afectados, se ha de

[227] Asunto C-28/08 P, entre la Comisión Europea y *Bavarian Lager Co Ltd*, resolviendo en Recurso de Casación.
En este asunto, la empresa cervecera *Bavarian Lager* presentó una denuncia en la Comisión contra Reino Unido por un caso de restricción cuantitativa a la importación, pues las empresas cerveceras británicas estaban obligadas a permitir que los titulares de establecimientos compraran una cerveza procedente de otra empresa cervecera, a condición de que estuviera envasada en barril. Esta norma se denomina comúnmente «*Guest Beer Provision*» (GBP); si bien la mayoría de las cervezas fabricadas fuera del Reino Unido se vendían en botellas. Se inició un expediente por incumplimiento y hubo una reunión en 1996 entre la Comisión con Reino Unido, tras la cual modificó la norma y se archivó el expediente. Pero *Bavarian Lager* había solicitado la asistencia a dicha reunión y le fue denegada, solicitando el acceso al acta de la misma, la cual le fue facilitada ocultando los datos personales de cinco personas que habían intervenido ya que las mismas no habían otorgado su consentimiento. Posteriormente *Bavarian Lager* volvió a pedir el acta completa y la Comisión se lo denegó, por lo que interpuso un recurso ante el Tribunal de Primera Instancia solicitando la anulación de esa Decisión de la Comisión. Mediante sentencia de 8 de noviembre de 2007, el Tribunal de Primera Instancia anuló la Decisión de la Comisión al considerar que la mera inscripción del nombre de los interesados en el listado de los participantes en una reunión en nombre de la entidad que representaban no suponía un perjuicio y no amenazaba la intimidad de esas personas.

denegar legítimamente la solicitud de acceso a un documento público que incluye datos de carácter personal sin ocultar, tal es un acta de una reunión de la Comisión.

2.3.3.4 La Carta de Derechos Fundamentales de la Unión Europea.[228]

La Carta de Derechos Fundamentales de la Unión Europea[229], firmada en Niza en 2000, reconoce por vez primera el derecho a la protección de datos como un Derecho fundamental: *"Artículo 8: 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".*

Si bien la Carta era un espléndido documento, no por ello tenía fuerza jurídica vinculante. Tal y como ya expusimos, necesitaba de una norma que se la otorgase. Se incorporó así a la fallida Constitución Europea[230] (artículo II-68[231] y artículo I-51[232]) a fin de dotarla de dicha fuerza, en idénticos términos al artículo 8 mencionado. Pero el intento quedó en fracaso cuando el proceso de aprobación de la Constitución Europea no llegó a formalizarse. Afortunadamente, el 12 de diciembre de 2007, la Carta[233] fue nuevamente proclamada en Estrasburgo, e incorporada al Tratado de Lisboa[234], formando parte pues del Derecho originario de la Unión.

---

[228] Sobre la Carta de Derechos Fundamentales, ver ALONSO GARCÍA, R y SARMIENTO, D, *La Carta de Derechos Fundamentales de la Unión Europea,* Aranzadi, Cizur Menor, Navarra, 2006.
[229] Carta de los Derechos Fundamentales. DO C 303 de 14/12/2007.
[230] DOUE C 310, de 16 de diciembre de 2004.
[231] Texto idéntico al art. 8 de la Carta.
[232] Art. I-51 Constitución Europea: *"Protección de datos de carácter personal 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. La ley o ley marco europea establecerá 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".*
[233] DOUE C 303, de 14 de diciembre de 2007.
[234] DOUE C 306, de 17 de diciembre de 2007.

La Jurisprudencia del Tribunal de Justicia de la Unión Europea que analiza e interpreta los casos al amparo del derecho fundamental a la protección de datos recogido como tal en la Carta es numerosa. Así, las Sentencias *Österreichischer Rundfunk* y otros[235]; *Google Spain*[236], *Ryneš*[237] y *Schrems*[238].

2.3.3.5 Propuesta del nuevo Reglamento General de Protección de Datos (RGPD).

La Directiva de 1995 supuso todo un hito histórico en la regulación del derecho a la protección de datos, pero 20 años después la evolución de la tecnología (redes sociales, *cloud computing, smartphones*…), el avance exponencial del flujo migratorio de datos, la violación de datos en el continente[239], la globalización de las

[235] STJUE de 20 de mayo de 2003. Casos acumulados C-465/00, C-138/01 y C-139/01. Apartado 68. *"Las disposiciones de la Directiva 95/46, en la medida en que regulan el tratamiento de datos personales que pueden atentar contra las libertades fundamentales y, en particular, contra el derecho a la intimidad deben ser interpretados a la luz de los derechos fundamentales que, según una reiterada jurisprudencia, forman parte de los principios generales del Derecho cuyo respeto garantiza el Tribunal de Justicia* (véase, en particular, la sentencia de 6 de marzo de 2001, *Connolly*/Comisión, C-274/99 P, Rec. p. I-1611, apartado 37).

[236] STJUE de 13 de mayo de 2014 (Gran Sala). Asunto C-131/12. Google vs AEPD y Mario Costeja. Apartado 68. *"El Tribunal de Justicia ya ha declarado que las disposiciones de la Directiva 95/46, en la medida en que regulan el tratamiento de datos personales que pueden atentar contra las libertades fundamentales y, en particular, contra el derecho a la intimidad, deben ser interpretadas a la luz de los derechos fundamentales que, según reiterada jurisprudencia, forman parte de los principios generales del Derecho cuyo respeto garantiza el Tribunal de Justicia y que están actualmente recogidos en la Carta (véanse, en particular, las sentencias Connolly/Comisión, C‑274/99 P, EU:C:2001:127, apartado 37, y Österreichischer Rundfunk y otros, EU:C:2003:294, apartado 68).*

[237] STJUE de 11 de diciembre de 2014. Asunto C-212/13.
Apartado 29: *"Teniendo en cuenta que las disposiciones de la Directiva 95/46, en la medida en que regulan el tratamiento de datos personales que puede vulnerar las libertades fundamentales y, en particular, el derecho a la intimidad o la protección de la vida privada, deben ser interpretadas a la luz de los derechos fundamentales recogidos en la citada Carta (véase la sentencia Google Spain y Google, EU:C:2014:317, apartado 68), la excepción prevista en el artículo 3, apartado 2, segundo guión, de dicha Directiva debe ser interpretada en sentido estricto".*

[238] STJUE de 6 de octubre de 2015, Asunto C-362/14.
Apartado 38: *"Se debe recordar previamente que las disposiciones de la Directiva 95/46, en cuanto regulan el tratamiento de datos personales, que puede vulnerar las libertades fundamentales y, en particular, el derecho al respeto de la vida privada, deben ser necesariamente interpretadas a la luz de los derechos fundamentales protegidos por la Carta (véanse las sentencias Österreichischer Rundfunk y otros, C‑465/00, C‑138/01 y C‑139/01, apartado 68; Google Spain y Google, C‑131/12, apartado 68, y Ryneš, C‑212/13, apartado 29)".*

[239] A modo de ejemplo, las revelaciones de *Edward Snowden* sobre el espionaje de los EEUU. Ver apartado 3.4.1.1.

relaciones humanas y comerciales y la digitalización de nuestra sociedad reclamaban la existencia de un marco normativo más adecuado a las actuales necesidades.

El 25 de enero de 2012, la Comisión adoptó su propuesta de Reglamento General de Protección de Datos (5853/12)[240] a fin de sustituir a la Directiva 95/46/CE, reforzando los derechos a la protección de datos de las personas físicas y mejorando las oportunidades para las empresas facilitando el libre flujo de los datos personales en el mercado único digital[241].

Los servicios de la Comisión, en el documento de evaluación de impacto, determinaban que existen tres grandes problemas: *"problema 1: obstáculos que la fragmentación, la inseguridad jurídica y la aplicación poco coherente de las normas suponen para las empresas y las autoridades públicas; problema 2: dificultades para que las personas físicas controlen sus datos personales; problema 3: lagunas e incoherencias de la protección de datos personales en el ámbito de la cooperación policial y judicial en materia penal"*[242].

El proceso legislativo europeo es un sistema que presenta notables garantías, y muy diferenciado del nacional en tanto que la formación de la voluntad política de la Unión Europea está formada por la de sus Estados miembros.

El procedimiento legislativo ordinario europeo consiste en la adopción conjunta por el Parlamento Europeo y el Consejo, a propuesta de la Comisión, de un reglamento, una directiva o una decisión. Como es sabido, inicialmente la Comisión elabora una propuesta sobre la medida que se desea adoptar, y lo hace a través del servicio de la Comisión encargado del área económica correspondiente. Este servicio consulta con expertos nacionales, si bien sus consultas no son vinculantes. El proyecto acordado se debate en el seno de la Comisión y finalmente es adoptado por mayoría simple. Posteriormente ese proyecto se presenta simultáneamente al Parlamento y al Consejo, así como a los Comités consultivos (Comité Económico y Social y/o Comité de las Regiones). Después el Parlamento debate la propuesta y propone

[240] Disponible en: http://eur-lex.europa.eu/legal-content/ES/AUTO/?uri=COM:2012:0011:FIN.
[241] Ver Agenda Digital Europea. Disponible en: http://ec.europa.eu/digital-agenda/.
[242] Documento de evaluación de impacto. Disponible en: http://eur-lex.europa.eu/legal-content/ES/AUTO/?uri=CELEX:52012SC0073.

enmiendas o lo acepta en su totalidad. Es la denominada primera lectura. Ese documento elaborado por el Parlamento con o sin enmiendas, lo transmite al Consejo. El Consejo puede aprobarlo (y finaliza el procedimiento legislativo) o adoptar su postura en primera lectura, es decir, elaborar su propuesta.

En tres meses, el Parlamento tiene en segunda lectura tres alternativas: aprobar (o no pronunciarse) la posición del Consejo – y se adoptaría el acto-, rechazarlo –no se adopta el acto- o aprueba enmiendas en el texto del Consejo, transmitiéndose dicho texto al Consejo y a la Comisión que dictaminarán sobre esas enmiendas. A partir de ahí el Consejo delibera sobre las enmiendas del Parlamento y puede aprobarlas todas –se aprueba el acto- (necesita mayoría cualificada si la Comisión ha emitido dictamen favorable y unanimidad si no lo ha hecho); o no las aprueba o no consigue la mayoría suficiente. En este momento comienza el Procedimiento de Conciliación. El Comité de Conciliación (formado por 27 miembros del Consejo y 27 del Parlamento) tendrá que alcanzar un acuerdo sobre los dos textos en segunda lectura. Si en seis semanas no se aprueba el texto se considerará el acto no adoptado. Pero si aprueban un acto conjunto en ese plazo el texto se someterá al Consejo (quien tendrá que aprobarlo por mayoría cualificada) y al Parlamento (quien tendrá que aprobarlo por mayoría simple). Si se aprueba se adopta el acto, si no finaliza el procedimiento legislativo[243].

A fecha 7 de noviembre de 2015, el proceso legislativo de aprobación del RGPD[244] ha pasado por las siguientes fases: transmisión de la Propuesta al Parlamento Europeo y al Consejo (27/01/2012)[245], Dictamen del Supervisor Europeo de Protección de Datos (07/03/2012)[246], Dictamen del Comité Económico y Social Europeo (23/05/2012)[247], Dictamen del Comité de las Regiones (10/10/2012)[248],

[243] Más información en *El ABC del Derecho de la Unión Europea*. DR. KLAUS-DIETER BORCHARDT. Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2011. Disponible en: http://bookshop.europa.eu/es/el-abc-del-derecho-de-la-uni-n-europea-pbOA8107147/

[244] Procedimiento 2012/0011/COD.
COM (2012) 11
Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)

[245] Disponible en: http://eur-lex.europa.eu/legal-content/ES/AUTO/?uri=COM:2012:0011:FIN

[246] Disponible en: http://eur-lex.europa.eu/legal-content/ES/AUTO/?uri=OJ:C:2012:192:TOC

[247] Disponible en: http://eur-lex.europa.eu/legal-content/ES/AUTO/?uri=OJ:C:2012:192:TOC

Debates en el Consejo (07/12/2012)[249]; (08/03/2013), (06/06/2013); (07/10/2013); (06/10/2013); (06/12/2013); (04/03/2014); Dictamen del Parlamento en primera lectura (12/03/2014)[250]; Debates en el Consejo (06/06/2014): Posición de la Comisión sobre enmiendas del Parlamento en primera lectura (10/06/2014) ; Debates en el Consejo (10/10/2014); Acuerdo político del Consejo (04/12/2014); Debates en el Consejo (04/12/2014); (13/03/2015); (15/06/2105)[251].

En estos momentos, cuando los tres textos ya se han dado a conocer[252], proceden las reuniones a tres bandas entre Comisión, Parlamento y Consejo (el famoso trílogo), cuyas reuniones comenzaron en junio de 2015, y en los que todos los implicados han manifestado su voluntad de cierre para finales de 2015[253]. Así lo confirmó también *Thomas Zerdick*, en el VII Foro de la Privacidad[254]. Adicionalmente a esas tres propuestas, el Supervisor Europeo de Protección de Datos ha formulado *motu propio* una propuesta recomendada, para que sirva de ayuda y orientación en las negociaciones del trílogo[255].

El Reglamento General de Protección de Datos incluye nuevas definiciones que no existían en la Directiva 95/46/CE, tales como los conceptos de violación de datos personales, datos genéticos, datos biométricos, datos de salud, establecimiento

[248] Disponible en: http://eur-lex.europa.eu/legal-content/ES/AUTO/?uri=OJ:C:2012:391:TOC

[249] Disponible en: http://europa.eu/rapid/pressReleasesAction.do?reference=PRES/12/509&format=HTML&aged=0&lg=es&guiLanguage=es.

[250] Disponible en: http://www.europarl.europa.eu/omk/sipade2?PUBREF=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//es.

[251] Disponible en: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/15/5176&format=HTML&aged=0&lg=es&guiLanguage=es

[252] Cuadro comparativo de los tres textos, hecho público por el Consejo: http://data.consilium.europa.eu/doc/document/ST-10391-2015-INIT/en/pdf.
En la primera columna aparece la propuesta de la Comisión, en la segunda la del Parlamento, en la tercera la del Consejo y en la cuarta se señalan cuáles son los textos idénticos en las tres instituciones.

[253] *THOMAS ZERDICK* es Subdirector de la Unidad de Protección de Datos de la Comisión Europea.

[254] VII Foro de la Privacidad. *Data Privacy Institute*. Madrid 22 de septiembre de 2015. Ponencia: *European Data Protection Reform*.

[255] El Supervisor Europeo de Protección de Datos creó a finales de julio de 2015 una aplicación móvil gratuita – EDPS- para dar a conocer a los ciudadanos las cuatro versiones del texto (las propuestas de la Comisión, el Parlamento y el Consejo, así como la recomendada por ellos a los colegisladores, comparándolas en cuatro columnas.

principal, representante, empresa, grupo de empresas, normas corporativas vinculantes, niño o autoridad de control.

En cuanto a los principios aumenta los ya descritos en el artículo 6 de la Directiva 95/46/CE, incluyendo los principios de transparencia, violación de datos personales, o minimización de datos. Establece también nuevas condiciones de licitud del tratamiento en datos de niños en los servicios de la sociedad de la información.

También los derechos de los interesados se verán incrementados por el nuevo RGPD, incluyéndose derechos como la obligación de ofrecer información transparente y de fácil acceso y comprensión; de arbitrar procedimientos y mecanismos para ejercer los derechos de los interesados; otorgar información adicional en la obligación de informar, derecho al olvido, derecho a la portabilidad de datos, o el derecho de oposición y elaboración de perfiles.

En relación a las figuras del responsable y encargado del tratamiento, se crean nuevas obligaciones y principios. Destacamos la inclusión del principio de responsabilidad y el principio de protección de datos desde el diseño y por defecto, la figura de los corresponsables, las obligaciones del encargado del tratamiento, la obligación de conservar la documentación de las operaciones de los tratamientos en lugar del deber de notificarlos a la autoridad de control, nuevas obligaciones en la seguridad de los datos, obligación de notificar la violación de datos personales, obligaciones del responsable y del encargado del tratamiento en cuanto a la evaluación de impacto anteriores a operaciones de tratamiento arriesgados, o las obligaciones de autorización y consulta a las Autoridades de control antes de realizar determinados tratamientos de datos.

El principio de responsabilidad responde en inglés al término *"accountabilty*", traducido también como rendición de cuentas, si bien el término va más allá. Realmente es un concepto en construcción pero que va dotando de contenido con la responsabilidad, con la rendición de cuentas y con la capacidad de poder demostrar que realmente se ha cumplido con la obligación impuesta. Ello supone que el responsable del tratamiento no sólo implementa medidas de seguridad sino que tiene que poder demostrar lo que ha hecho, por lo que en este proceso se verá implicada

toda la organización, haciéndose obligatoria una cultura y formación en materia de protección de datos en todas las instancias de la sociedad.

El principio de protección de datos por diseño o por defecto (en inglés *by design* o *by default*), supone que el responsable del tratamiento tiene la obligación de poner en funcionamiento con carácter previo al tratamiento de los datos todas las medidas y procedimientos que garanticen que éste se vaya a realizar conforme establece el Reglamento. Estos mecanismos tendrán también la obligación de garantizar que sólo serán objeto de tratamiento los datos necesarios para el fin determinado, y que no se conserven datos más allá de lo necesario para estos fines, siendo además que el acceso estará limitado a un número de personas. Esta obligación supone un toque de atención a las empresas desarrolladoras de software que deberán diseñar sus productos para el cumplimiento de estas obligaciones.

Además, desaparece la obligación de notificar los ficheros a la Autoridad de control. Esta acción, que tanto trabajo ha dado a los especialistas en protección de datos, suponía al menos la primera toma de contacto del responsable del fichero para que comenzara a cumplir con las obligaciones en materia de protección de datos. Inculcar una política adecuada de protección de datos en las empresas ha sido tarea ardua y agotadora que aún está iniciando su camino. Pocas son las empresas que ha cumplido con sus obligaciones por entender la filosofía del valor del derecho fundamental de las personas. Las razones para su implementación han sido fundamentalmente económicas; el miedo a una sanción de la Autoridad de control. La norma vigente hasta ahora (la Directiva 95/46/CE) centra la atención en la tutela del dato personal en su origen, en la recogida, pero la evolución de la tecnología y el tráfico de datos diario de cada uno de nosotros (pensemos en cuántos datos a título personal enviamos cada día por ejemplo con el simple uso de los *smartphones* y sus aplicaciones) ha desplazado la atención y la protección a los usos de los datos y a los riesgos que cada uso conlleva.

Con el nuevo Reglamento, el encargado del tratamiento se verá obligado a documentar todos los tratamientos de datos que efectúe, no siendo necesaria su notificación a priori a la Autoridad de control. Esta obligación, que ciertamente

supone una garantía, en la práctica va a suponer una impresionante carga de trabajo para los responsables.

La gran novedad que supondrá un cambio cualitativo en las medidas de cumplimiento de la seguridad son sin lugar a dudas las evaluaciones de impacto, los conocidos PIA (*Privacy Impact Assesment*), los cuales serán necesarios para todas aquellas operaciones que supongan un riesgo para el derecho fundamental. Concretamente, la propuesta de Reglamento presentada por la Comisión dice en su artículo 33 que "*cuando las operaciones de tratamiento entrañen riesgos específicos para los derechos y libertades de los interesados en razón de su naturaleza, alcance o fines, el responsable o el encargado del tratamiento que actúe por cuenta del responsable llevarán a cabo una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales*". Las enmiendas formuladas en los textos del Parlamento y Consejo detallan más aún esta obligación. A pesar de que el futuro Reglamento señala algunos supuestos en los que serán obligatorias dichas evaluaciones de impacto[256], es ese listado meramente enunciativo y no limitativo, por lo que desde el punto de vista jurídico nos encontramos ante un concepto –el del riesgo- indeterminado que entendemos generará muchas controversias viéndose los organismos de control así como los judiciales en la obligación de interpretarlos.

[256] Artículo 33.2 RGPD, texto propuesto por la Comisión: *"Las siguientes operaciones de tratamiento, en particular, entrañan los riesgos específicos contemplados en el apartado 1: a) la evaluación sistemática y exhaustiva de los aspectos personales propios de una persona física o destinada a analizar o a predecir, en particular, su situación económica, localización, estado de salud, referencias personales, fiabilidad o comportamiento, que se base en un tratamiento automatizado y sobre la base de la cual se tomen medidas que produzcan efectos jurídicos que atañan o afecten significativamente a dicha persona; b) el tratamiento a gran escala de información sobre la vida sexual, la salud, la raza y el origen étnico o destinada a la prestación de atención sanitaria, investigaciones epidemiológicas o estudios relativos a enfermedades mentales o infecciosas, cuando los datos sean tratados con el fin de tomar medidas o decisiones sobre personas concretas; c) el seguimiento de zonas de acceso público, en particular cuando se utilicen dispositivos optoelectrónicos (videovigilancia) a gran escala; d) el tratamiento de datos personales en ficheros a gran escala relativos a niños, o el tratamiento de datos genéticos o biométricos; e) otras operaciones de tratamiento para las cuales sea necesaria la consulta de la autoridad de control con arreglo a lo dispuesto en el artículo 34, apartado 2, letra b)".*
Artículo 33.3 RGPD, texto propuesto por la Comisión: *"La evaluación deberá incluir, como mínimo, una descripción general de las operaciones de tratamiento previstas, una evaluación de los riesgos para los derechos y libertades de los interesados, las medidas contempladas para hacer frente a los riesgos, y las garantías, medidas de seguridad y mecanismos destinados a garantizar la protección de datos personales y a probar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas".*

En esta línea de análisis de riesgos y estandarización de procedimientos se hace imprescindible y muy importante la labor que habrán de desarrollar los Delegados de Protección de Datos, más conocidos como DPO (*Data Protection Officer*), tanto en empresas públicas como privadas. Este punto del texto está siendo uno de los más discutidos, donde las enmiendas formuladas por el Parlamento y el Consejo difieren entre sí, y donde la labor de los lobbies[257] es muy intensa. El Delegado de Protección de Datos será independiente, y sólo podrá ser relevado de su trabajo por incumplimiento del mismo. En cuanto a la obligatoriedad del DPO los textos presentados por las tres instituciones difieren. Parece que será obligatorio para las empresas públicas, mientras está por determinar los requisitos que deberán tener las empresas privadas para que les sea exigible dicha figura: mientras que para la Comisión el criterio han de ser el número de trabajadores de la empresa (250), para el Parlamento lo será el número de afectados en la empresa (5000). Veremos cuál será el criterio final. Lo que es indudable es el relevante papel que va a tener el Delegado de Protección de Datos, que será el enlace entre la empresa y las Autoridades de control y el encargado de despertar la cultura de protección de datos allá donde se encuentre. También el DPO será el encargado de notificar tanto a las Autoridades de control como a los interesados las violaciones del derecho debidas a una brecha de seguridad. Mucho y nuevo trabajo para el DPO, cuyo perfil también está aún por definir.

Son también destacables en el nuevo Reglamento General de Protección de Datos la incorporación de códigos de conducta, mecanismos de certificación y sellos de protección de datos.

[257] En Bruselas existen la mayor concentración de lobbies o grupos de presión del mundo después de Washington, que promueven los intereses de las grandes empresas e intentan influir en la toma de decisiones de la UE. La presencia de estos grupos es considerada una actividad legítima y necesaria en el proceso de toma de decisiones, que garantiza que las políticas de la UE respondan a las necesidades reales de los ciudadanos. Para que ese proceso sea transparente se creó por la Comisión Europea el Registro de Transparencia de la UE, el cual permite un control adecuado y garantiza que las instituciones de la Unión rindan cuentas de su actuación. Abarca todas las actividades que tienen por objeto influir, directa o indirectamente, en la definición y aplicación de políticas. En Octubre de 2015 hay inscritas más de 8.000 entidades.
Es curioso observar en el propio Parlamento Europeo cómo hay una zona designada donde celebrar las reuniones con los lobbies.
Para mayor información:
http://ec.europa.eu/transparencyregister/public/staticPage/displayStaticPage.do?locale=es&reference=WHOS_IS_EXPECTED_TO_REGISTER

En cuanto al discutido e importante asunto que es la transferencia de datos personales a terceros países u organizaciones internacionales, establece el Reglamento los criterios que ha de tener en cuenta la Comisión para adoptar Decisiones relativas a la adecuación del nivel de protección de datos, siendo estos la exigencia a los terceros del Estado de Derecho, de la existencia de un recurso jurisdiccional así como la de una supervisión independiente. Para aquellos terceros para los que no haya Decisión acordada, se requerirá la existencia de cláusulas tipo de protección de datos, normas corporativas vinculantes o cláusulas contractuales.

Las Autoridades de control también tendrán mayor trabajo con la nueva normativa, pues además de todas las competencias que ahora tienen (al menos en España) se incorporarán otras que vendrán especialmente por los análisis de riesgo de los tratamientos así como por los mecanismos de cooperación y de coherencia. La cooperación se refiere a la asistencia recíproca obligatoria así como las operaciones conjuntas; y en cuanto al mecanismo de coherencia ya se han vertido litros de tinta. Este procedimiento será llevado a cabo por el Consejo Europeo de Protección de Datos (CEPD), organismo que sustituye al Grupo de Trabajo del Artículo 29. Describe el RGPD su independencia, actividades, la obligatoriedad de informes anuales, la existencia de un reglamento interno y las funciones del Presidente. La Secretaría del CEPD será llevada a cabo por el Supervisor Europeo de Protección de Datos.

En cuanto a los recursos judiciales es interesante resaltar la posibilidad que otorga el Reglamento a los interesados que se vean afectados por una decisión de una Autoridad de control de un Estado miembro en el que no tienen su residencia habitual de solicitar a la autoridad de control del Estado miembro en el que sí tiene su residencia habitual que ejercite en su nombre una acción contra la Autoridad de control competente en el otro Estado miembro. También se refiere el Reglamento General de Protección de Datos al derecho de indemnización tanto por el responsable como por los corresponsables y coencargados del tratamiento.

Dispone el Reglamento obligaciones específicas impuestas a los estados para adoptar excepciones cuando haya que conciliar el derecho a la protección de datos y el

derecho a la libertad de expresión; para adoptar leyes específicas para el tratamiento de datos en el contexto del empleo o condiciones específicas del tratamiento de datos para fines históricos, estadísticos y de investigación científica.

2.4 Autoridades europeas en protección de datos.

Tal y como hemos ido viendo en este capítulo, a medida que el reconocimiento al derecho de la protección de datos se ha ido configurando normativamente, en paralelo se regulaba también sobre las distintas Autoridades de control u organismos consultivos que debían tutelar y asesorar en el cumplimiento de la norma y el ejercicio de los derechos por parte de los ciudadanos. Nos encontramos con tres niveles de órganos: los Órganos Consultivos y Grupos de Trabajo, las Autoridades de Control, y un tercer nivel intermedio en el que incluiremos Órganos de coordinación con capacidad de dictar resoluciones vinculantes[258].

2.4.1 Órganos Consultivos y Grupos de Trabajo.

2.4.1.1 Comité Consultivo del Convenio 108.

El Convenio 108 del Consejo de Europa[259] tiene por objeto 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 («protección de datos»)[260].

Es en este instrumento donde por vez primera se creó un órgano (con representación de todos los Estados miembros) con funciones específicas en materia de protección

[258] Ver REBOLLO DELGADO, L. *Derechos Fundamentales y Protección de Datos*, Dykinson, Madrid, 2004.
[259] Consejo de Europa. Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. CETS nº 108, Estrasburgo 1981.
[260] Art. 1 Convenio 108.

de datos, sin funciones de control, pero sí con múltiples tareas para elaborar documentos de ayuda, propuestas de mejora y enmiendas.

Las funciones del Comité Consultivo en el actual Convenio 108 son[261]:

- Presentar propuestas con el fin de facilitar o de mejorar la aplicación del Convenio;
- presentar propuestas de enmienda del Convenio;
- formular su opinión acerca de cualquier propuesta de enmienda presentada por una parte o por el Consejo de Ministros;
- expresar, a petición de una Parte, su opinión acerca de cualquier cuestión relativa a la aplicación del Convenio.

Pero el borrador del nuevo Convenio le otorga más competencias al Comité, situándolo como un organismo mediador en la medida que puede actuar para resolver de forma amistosa los conflictos generados en la aplicación del Convenio; le faculta para desarrollar o aprobar modelos de garantías estandarizadas y preparar, antes de cualquier nueva adhesión al Convenio, un dictamen en relación con el nivel de protección de datos personales del Estado candidato a la misma y, en caso necesario, deberá recomendar las medidas a tomar por dicho candidato para alcanzar el cumplimiento de las disposiciones del Convenio.

La actividad del Comité, desde sus inicios, se ha ido plasmando en informes, opiniones y estudios[262], además de documentos de Recomendaciones del Comité de Ministros del Consejo sobre cuestiones específicas de la materia, como las redes sociales, la creación de perfiles o el ámbito laboral.[263] Es el Comité Consultivo el alma mater del Consejo de Europa en materia de protección de datos. Ha sido visionario en la necesidad de modernizar la regulación y las relaciones de los estados con los ciudadanos. De hecho, fue en 2010 cuando inició todo el proceso de modernización que ha dado origen a un Convenio revisado, pendiente de su cierre,

[261] Artículo 19 Convenio 108.
[262] Para mayor detalle, es interesante consultar la web del Consejo de Europa: http://www.coe.int/t/dghl/standardsetting/dataprotection/docrep_en.asp.
[263] Disponible en: http://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp.

muy trabajado y que ha sido base de todos los cambios normativos actuales en protección de datos, tanto a nivel de Europa como de la OCDE, tal y como se ha venido exponiendo en este trabajo.[264]

La agenda de trabajo del Comité Consultivo para los años 2014 y 2015 tiene varios ítems, entre ellos la modernización del Convenio 108 y su implementación y modernización; la revisión de Recomendaciones y Textos ya existentes[265] y la promoción de la cultura y conocimiento de la protección de datos, a la vez que seguir dando a conocer el Día de la Protección de Datos en Europa que desde 2006 se celebra el 28 de enero, día en que se conmemora la firma del Convenio 108, y que impulsó, junto con la Comisión Europea y las Autoridades de Protección de Datos de los Estados miembros de la Unión Europea. Es de resaltar, por sus implicaciones prácticas y de defensa del derecho, el trabajo realizado por el Comité en la propuesta de formalización del derecho a la protección de datos como derecho fundamental, mediante instrumento propio del Consejo de Europa, de modo que se garantizara el acceso al Tribunal Europeo de Derechos Humanos (TEDH).

Organizativamente, el Comité está formado por un representante y un suplente de cada estado parte del Convenio. Tiene una Oficina (*Bureau*) cuya dirección es llevada a cabo por un Presidente, dos Vicepresidentes, cuatro miembros más y el Presidente saliente, todos ellos elegidos de entre los miembros[266]. La Oficina posee además una Secretaría General. Todos los Estados miembros del Consejo de Europa que no sean parte del Convenio pueden estar representados por un observador y, mediante decisión unánime, se podrá invitar como observador a un estado no miembro. También podrán ser observadores representantes de varios organismos del Consejo de Europa, tales como de la Asamblea Parlamentaria, el Congreso de los Poderes Locales y Regionales, el Tribunal Europeo de Derechos Humanos, la Comisión de Derechos Humanos, la Conferencia de las Organizaciones No

[264] Nos remitimos en cuanto al proceso de modernización a todo lo expuesto en el apartado 2.1.

[265] *Recommendation (87) 15 regulating the use of personal data in the police sector, Recommendation (89) 2 on the protection of personal data used for employment purposes, Recommendation (97) 5 on the protection of medical data, Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data*.

[266] Las funciones del *Bureau* están descritas en el apartado 3 del artículo 10 bis de las Reglas de Procedimiento. Ver 267.

Gubernamentales reconocidas en el Consejo de Europa, el Comité Director de Derechos Humanos, el Comité Europeo de Cooperación Jurídica, el Comité Europeo de Problemas Penales y el Comité Directivo sobre los nuevos servicios de comunicación.

Las reglas de procedimiento actuales del Comité Consultivo del Convenio 108 son de 2014, y están recogidas en un documento publicado en la página web del Consejo de Europa[267].

2.4.1.2 Agencia Europea de los Derechos Fundamentales de la Unión Europea (FRA).[268]

La Agencia Europea de los Derechos Fundamentales se crea al amparo del Reglamento (CE) núm. 168/2007 del Consejo[269].

Su objetivo[270] es proporcionar a las instituciones, órganos, organismos y agencias competentes de la Comunidad y a sus Estados miembros cuando apliquen el Derecho comunitario asistencia y asesoramiento en materia de derechos fundamentales con el fin de ayudarles a respetarlos plenamente cuando adopten medidas o establezcan líneas de actuación en sus esferas de competencia respectivas. Se encarga de recoger y difundir información sobre los derechos fundamentales y asesora sobre cómo fomentarlos.

Se creó en el año 2007 para sustituir al Observatorio Europeo del Racismo y la Xenofobia, y su sede está en Viena (Austria).

Los cometidos de la Agencia, que deben cumplirse dentro de los límites de los ámbitos temáticos, incluyen: la recopilación, el análisis, la difusión y la evaluación,

[267] Disponible en: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2014)Rules_Internal_rules%20of%20T-PD_En_Sept_2014.pdf.
[268] *Fundamental Rights Agency.*
[269] Reglamento (CE) 168/2007 del Consejo, de 15 de febrero de 2007, por el que se crea una Agencia de los Derechos Fundamentales de la Unión Europea. DOUE L 53, de 22 de julio de 2007.
[270] Artículo 2 del Reglamento (CE) núm. 168/2007 del Consejo.

con total independencia, de los datos e información pertinentes, objetivos, fiables y comparables sobre los efectos concretos de las medidas adoptadas por la UE en los derechos fundamentales, y sobre las buenas prácticas en materia de respeto y fomento de tales derechos; el desarrollo de normas para mejorar la comparabilidad, objetividad y fiabilidad de los datos a escala europea, en cooperación con la Comisión y los Estados miembros; la realización de investigaciones y trabajos científicos, estudios preparatorios y de viabilidad; la formulación y publicación de conclusiones y dictámenes sobre temas específicos y sobre la evolución de los derechos fundamentales en la ejecución de las políticas, dirigidos a las instituciones europeas y a los Estados miembros en el marco de la aplicación del Derecho comunitario; la publicación de un informe anual sobre las cuestiones relativas a los derechos fundamentales derivadas de los sectores de actividad de la Agencia; la publicación de informes temáticos basados en sus análisis; la publicación de un informe de actividad anual; el desarrollo de una estrategia de comunicación, y el fomento del diálogo con la sociedad civil, con el fin de sensibilizar a la opinión pública sobre los derechos fundamentales.

La Agencia mantiene también relaciones institucionales estrechas a nivel internacional, europeo y nacional, cuyo objetivo es cooperar y evitar duplicaciones de trabajo.

Está formada por un Consejo de Administración (órgano de programación y vigilancia), un Consejo Ejecutivo, un Comité Científico y un Director. El Consejo puede decidir invitar a participar en los trabajos de la Agencia a los países que hayan suscrito un acuerdo de estabilización y asociación con la UE. De este modo, facilita la paulatina adaptación de la legislación de estos países al Derecho comunitario, y los apoya en su esfuerzo hacia la integración europea.

En el último informe anual publicado, de junio de 2015, insta a los Estados miembros a aprobar un marco uniforme en materia de protección de datos y resalta la

importancia de las Autoridades de control y del inexorable requisito de cumplimiento real y efectivo de la independencia que éstas deben tener.[271]

2.4.1.3 El Comité de las Regiones (CDR).

El Comité de las Regiones es un organismo consultivo que representa a los entes regionales y locales de Europa, es la Asamblea de la Unión Europea de los representantes nacionales y locales.[272] Con sede en Bruselas, se creó en 1994 y está formado por 350 miembros procedentes de los 28 estados miembros, teniendo que ser todos ellos cargos con representación en sus países. La creación de este órgano consultivo fue prevista en el antiguo Tratado Constitutivo de las Comunidades Europeas[273] y actualmente su existencia y descripción se encuentran recogidos en los artículos 300, 305, 306 y 307 del Tratado de Funcionamiento de la Unión Europea.

La principal función del Comité de las Regiones es permitir a las regiones y ciudades participar formalmente en la elaboración de la legislación de la Unión Europea, garantizando así el respeto a las posiciones de los entes regionales y locales. De hecho, si en la elaboración de una norma de determinadas materias[274] no se les consulta pueden llevar el asunto ante el TJUE.

En materia de protección de datos se ha pronunciado en diversas ocasiones a través de dictámenes e incluso con publicaciones. En cuanto al nuevo Reglamento General de Protección de Datos, el Comité de las Regiones elaboró un Dictamen acerca del paquete sobre la protección de datos[275] en el que celebraba las propuestas, si bien consideraba más conveniente otorgar un mayor poder de decisión a los Estados miembros.

[271] Disponible en: http://fra.europa.eu/sites/default/files/fra-annual-report-2014_en.pdf.
[272] Declaración de misión del CDR. Disponible en: http://cor.europa.eu/en/about/Documents/Mission%20statement/ES.pdf.
[273] Artículos 263, 64 y 265 del Tratado Constitutivo de las Comunidades Europeas.
[274] Administración local y regional, como la sanidad, la educación, el empleo, la política social, la cohesión económica y social, el transporte, la energía y el cambio climático.
[275] CDR 625/2012. DO C 391.

2.4.1.4 El Comité Económico y Social Europeo (CESE).

El Comité Económico y Social Europeo es un órgano consultivo más de la Unión Europea compuesto por representantes de las organizaciones de trabajadores y empresarios y otros grupos de interés, que nació en 1957. Su existencia viene avalada por el artículo 300 del Tratado de Funcionamiento de la Unión Europea[276]

Al igual que el Comité de las Regiones, elabora Dictámenes para las instituciones de la UE como son la Comisión Europea, el Consejo y el Parlamento, y actúa como puente entre las instituciones de la UE con capacidad decisoria y los ciudadanos europeos emitiendo su opinión sobre las propuestas legislativas. También elaboran dictámenes de motu propio sobre temas que considera de interés.

Tiene tres tareas principales: velar porque la política y la legislación de la UE se adapten a las condiciones económicas y sociales, buscando un consenso que sirva al bien común; promover una Unión Europea participativa, dando voz a las organizaciones de trabajadores y empresarios y otros grupos de interés y garantizando el diálogo con ellos; y promover los valores de la integración europea e impulsar la causa de la democracia participativa y las organizaciones de la sociedad civil.[277]

Las opiniones vertidas por el CESE en sus Dictámenes han sido numerosas en materia de protección de datos[278]. Hemos de resaltar el Dictamen sobre la Propuesta de Reglamento General de Protección de Datos[279], el cual es bastante extenso si lo comparamos con el del Comité de las Regiones. Valora la iniciativa, pero describe algunos asuntos de mayor relevancia (en especial las concernientes a la descripción

[276] Artículos 300 a 305 TFUE, antiguos 258 A 262 del Tratado Constitutivo de las Comunidades Europeas.
[277] Disponible en: http://europa.eu/about-eu/institutions-bodies/eesc/index_es.htm
[278] Disponible en: https://dm.eesc.europa.eu/eescdocumentsearch/Pages/opinionsresults.aspx?k=data%20protection
[279] CESE 1303/2012, AC SOC /455. Ponente Pegado Liz, aprobado el 23/05/2012.

de tecnologías y sistemas de recolección de datos) que debieran ser recogidos en el texto. Asimismo muestra su disconformidad con algunos asuntos en los que propone soluciones concretas y otros en los que su posición es más indeterminada. Así por ejemplo propone recoger en el texto la posibilidad de ejercer la acción de indemnización en grupo, habilitando para ello un instrumento judicial armonizado a nivel de Europa. Su posición es más ambigua en asuntos como las condiciones que han de cumplirse para exigir la obligación de tener un Delegado de Protección de Datos[280].

[280] Para mayor detalle, consultar el documento en https://dm.eesc.europa.eu/eescdocumentsearch/Pages/opinionsresults.aspx?k=data%20protection.

2.4.1.5 Grupo de Telecomunicaciones de Berlín.[281]

Más conocido como Grupo de Berlín, el *International Working Group on Data Protection in Telecommunications* (IWGDPT) nació en 1983, en el seno de la Conferencia Internacional de Comisarios de Protección de Datos y Privacidad, gracias a la iniciativa del Comisario de Berlín para la Protección de Datos, el cual preside el Grupo. Reúne a Autoridades de control de países europeos y de América del Norte, además de representantes de organizaciones internacionales y expertos. Es un foro de trabajo que debate sobre las implicaciones del uso de las

[281] Sus informes pueden consultarse en http://www.datenschutz-berlin.de.
Documentos de trabajo más recientes:

- Sobre la privacidad y *Wearable Computing* Dispositivos (Seúl, 27/28. 04 2015).
- Transparencia de Información: la rendición de cuentas. (Seúl, 27/28 de abril 2015).
- Privacidad y riesgos de seguridad con el uso de "Dispositivos propios" en Redes Corporativas (Berlín, 14/15. 10 2014).
- Datos y Privacidad de Big Data. (Skopje, 5. / 6. Mai 2014).
- Privacidad y la vigilancia aérea (Berlín, 2/3. 09 2013).
- El Derecho Humano a las Telecomunicaciones Secretas (Berlín, 2/3. 09 2013).
- Papel y Recomendaciones sobre la publicación de datos personales en la web, sitio web de contenido, Indexación y la protección de la privacidad de Trabajo (15. / 16. Abril 2013, Praga (República Checa)).
- Seguimiento del Web y privacidad: El respeto por el contexto, la transparencia y el control sigue siendo esencial (15. / 16 abril de 2013, Praga (República Checa).)
- Cloud Computing - Privacidad y protección de datos cuestiones. (Sopot (Polonia), 23/24 abril de 2012).
- Privacidad por Diseño y Medición inteligente: Minimizar información personal para mantener la privacidad (Berlín, 12/13 septiembre de 2011.).
- Privacidad y Micropagos electrónicos en Internet (Berlín, 12/13. Septiembre de 2011).
- Registradores de datos de eventos (EDR) en los vehículos / Privacidad y protección de datos problemas para los gobiernos y fabricantes (Montreal (Canadá) 4-5 abril de 2011).
- Procesamiento móvil de Datos de Carácter Personal y Seguridad (Berlín, 6/7. Septiembre de 2010).
- Utilización de inspección profunda de paquetes para fines de marketing (Berlín, 6/7. Septiembre de 2010).
- La Carta de Granada de la privacidad en el mundo digital (Granada (España), 15/16. Abril de 2010).
- Privacidad, riesgos en la reutilización de las cuentas de correo electrónico y servicios de la sociedad de información similares (Berlín, 7/08/09/2009 - revisado y actualizado Granada (España) 15. / 16 abril de 2010.).
- Recomendación sobre la protección de datos y *E-Waste* (Sofía (Bulgaria), 12. / 03.13.2009).
- Informe y Orientaciones sobre *Road Pricing* - "Memorándum de Sofía"-(Sofía (Bulgaria), 12./03.13.2009).
- Informe y Orientaciones sobre privacidad en las redes sociales-"Roma Memorándum" - (Roma (Italia), 3. / 03.04.2008).
- Recomendación sobre la Implementación y Aplicación de la Convención del Consejo de Europa, N ° 185 sobre la Ciberdelincuencia (también conocido como "Convenio de Budapest") (Roma (Italia), 3. / 03.04.2008).

telecomunicaciones en la esfera privada de los individuos, teniendo sus documentos de trabajo un valor práctico importante por cuanto se profundiza en el impacto de las distintas tecnologías, siendo este punto clave en el desarrollo de la normativa de protección de datos. Desde principios de los años 90 el Grupo ha venido teniendo especial atención a la privacidad en Internet.

2.4.1.6 Grupo de Trabajo del Artículo 29 (GT 29).[282]

El Grupo del Trabajo del Artículo 29 fue creado por la Directiva 95/46/CE[283]. Es un órgano consultivo de carácter independiente formado por las Autoridades de Protección de Datos de todos los Estados miembros, la Comisión Europea (que desempeña la función de Secretaría) y el Supervisor Europeo de Protección de Datos[284]. Los países candidatos a ser miembros de la Unión así como los países miembros del EEE también pueden acudir a las reuniones, si bien sólo en calidad de Observadores. Elabora anualmente un informe sobre la situación de la protección de las personas físicas en cuanto a tratamiento de datos se refiere, tanto en la Unión Europea como en países terceros; informe que transmite al Parlamento Europeo, al Consejo y a la Comisión[285].

El objetivo fundamental del Grupo de Trabajo del artículo 29 ha sido siempre contribuir a la homogeneización de las distintas normativas en materia de protección de datos en los Estados miembros, y ello porque si bien la Directiva es de aplicación a toda la Unión Europea también es cierto que cada país la ha traspuesto según su normativa y conveniencia, lo que ha producido divergencias en la aplicación. Por ello, una de las principales funciones que el artículo 30 de la Directiva 95/46/CE le

[282] Toda la información acerca del GT 29 está disponible en: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.

[283] Directiva 95/46/CE, de 24 de octubre, 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 (DOCE L 281, de 23 de noviembre).

[284] Artículo 29 Directiva 95/46/CE: *"Se crea un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, en lo sucesivo denominado « Grupo ». Dicho grupo tendrá carácter consultivo e independiente".*

[285] Disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/annual-report/index_en.htm

otorga al GT 29 es estudiar todo lo relativo a la aplicación de las disposiciones nacionales respecto de la Directiva para contribuir a esa homogeneización a la que nos referíamos. También dispone otras funciones tales como emitir dictámenes a la Comisión sobre el nivel de protección tanto en la Comunidad como en países terceros; asesorarla sobre cualquier proyecto de modificación de la Directiva o sobre cualquier otro proyecto comunitario que afecte a la protección de datos personales; emitir dictámenes sobre los códigos de conducta a nivel comunitario o formular recomendaciones sobre cualquier asunto relacionado con la protección de las personas en lo que respecta al tratamiento de datos personales en la Unión Europea. Asimismo, el Grupo debe informar a la Comisión de la existencia de divergencias entre la legislación y la práctica de los Estados miembros que pudieran afectar a la equivalencia de la protección de las personas.

También el artículo 15 de la Directiva 2002/58/CE, sobre la Privacidad y las comunicaciones electrónicas[286], dota de competencia al Grupo para ejercer las funciones descritas en el artículo 30 de la Directiva 95/46/CE en los asuntos específicos de esa Directiva, es decir, la protección de los derechos y las libertades fundamentales y de los intereses legítimos en el sector de las comunicaciones electrónicas.

Las reglas de procedimiento del GT29 están recogidas en un documento elaborado por el propio Grupo[287] (la iniciativa de los borradores, quiénes pueden asistir a las reuniones, el quorum necesario, cómo se toman las decisiones, quiénes serán los redactores, el reparto de las intervenciones, etc). Teniendo en cuenta que el número de Estados miembros aumentó de 15 a 28, es un dato a reflexionar sobre la eficacia de un organismo flexible y cambiante. La mayoría de las opiniones y documentos se adoptan por consenso, aunque cuando es necesaria una votación formal el quorum es de mayoría simple. El Presidente es elegido por los miembros del Grupo y

[286] Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. DO L 201 de 31.7.2002, p. 37-47.

[287] Para consultar el documento, ver: http://ec.europa.eu/justice/data-protection/article-29/files/rules-art-29_en.pdf.

desempeña un papel destacado, fijando las prioridades y definiendo con la Secretaría de la Comisión el orden del día de las reuniones.

La Secretaría del Grupo del Artículo 29 la lleva la Comisión, actualmente la Dirección General de Justicia y Consumidores, Unidad de Protección de Datos. Las reuniones son celebradas en la Comisión, en Bruselas, incluyendo la Conferencia Anual de la Protección de Datos Europea y la Conferencia Internacional de Protección de Datos.

No se debe confundir el papel del Grupo de Trabajo con el del Comité que establece el artículo 31 de la Directiva 95/46/CE[288], formado este último por representantes de los gobiernos, y cuya función es asistir a la Comisión. El Comité tiene poder de decisión, mientras que el Grupo de Trabajo tan sólo tiene carácter consultivo. *"La Comisión únicamente puede adoptar las medidas propuestas si éstas son conformes con el dictamen del Comité, en el caso de que éste no fuera favorable, la Comisión deberá acudir directamente al Consejo…*"[289]

La labor del GT29 ha sido extraordinaria e intensa. Desde su creación hasta octubre de 2015 ha publicado casi 230 documentos (entre opiniones, recomendaciones y otros documentos) para ayudar a unificar criterios en materia de protección de datos[290]. Destacamos algunos documentos recientes, tales como el Dictamen

[288] Artículo 31 Directiva 95/46/CE: *"El Comité. 1. La Comisión estará asistida por un Comité compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión. 2. El representante de la Comisión presentará al Comité un proyecto de las medidas que se hayan de adoptar. El Comité emitirá su dictamen sobre dicho proyecto en un plazo que el presidente podrá determinar en función de la urgencia de la cuestión de que se trate. El dictamen se emitirá según la mayoría prevista en el apartado 2 del artículo 148 del Tratado. Los votos de los representantes de los Estados miembros en el seno del Comité se ponderarán del modo establecido en el artículo anteriormente citado. El presidente no tomará parte en la votación. La Comisión adoptará las medidas que serán de aplicación inmediata. Sin embargo, si dichas medidas no fueren conformes al dictamen del Comité, habrán de ser comunicadas sin demora por la Comisión al Consejo. En este caso: — la Comisión aplazará la aplicación de las medidas que ha decidido por un período de tres meses a partir de la fecha de dicha comunicación; — el Consejo, actuando por mayoría cualificada, podrá adoptar una decisión diferente dentro del plazo de tiempo mencionado en el primer guion".*

[289] "El derecho a la intimidad en la nueva ley orgánica de protección de datos". Ana Isabel Herrán Ortiz. Dykinson 2002. P. 193.

[290] Los documentos de trabajo del GT29 pueden ser consultados en: http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm

02/2015, sobre Código de Conducta del C-SIG[291] sobre Cloud Computing[292]; Dictamen 01/2015 sobre la privacidad y la protección de datos en relación con la utilización de drones[293]; Documento explicativo sobre normas corporativas vinculantes para los encargados del tratamiento[294]; Declaración conjunta de las Autoridades de protección de datos (sobre los valores en Europa sobre la protección de datos)[295]; Directrices sobre la aplicación del derecho al olvido a raíz de la sentencia Google España vs Agencia Española de Protección de Datos[296] o el Dictamen 8/2014 sobre los desarrollos recientes en el Internet de las Cosas[297].

Tal y como reconoce *Yves Poullet*[298], más allá del marco institucional y normativo, existe un enfoque estratégico[299] en el Grupo del Artículo 29 para dotarlo de mayor visibilidad e impacto en sus cometidos. En primer lugar, entiende *Poullet* que hay una estrategia de alianzas entre la Unión Europea y otros actores, como la Comisión o el Supervisor Europeo de Protección de Datos. La Comisión no sólo provee la Secretaría del Grupo, sino que además ha de tener en cuenta su opinión, lo cual supone que se generen sinergias entre ambos. A pesar de esta afirmación, que es casi un dato objetivo, (y se ha visto claramente por ejemplo en la posición de ambos en la

[291] Cloud Select Industry Group.

[292] Disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf

[293] Disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf

[294] Disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp204.rev_en.pdf

[295] Disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp227_en.pdf

[296] Disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf

[297] Disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.
En relación al IoT, GARCÍA SÁNCHEZ, M. Internet de las Cosas: Implicaciones en protección de datos. Conferencia impartida en la Universidad Internacional Menéndez Pelayo en Santander, dentro del curso "Retos de Protección de Datos en las sociedades actuales", julio 2015.
AREITIO BERTOLÍN, J**.** *Protección de la seguridad y privacidad en la internet de los objetos (IoT) y su correlación con RFID*. Eurofach electrónica: actualidad y tecnología de la industria electrónica, núm. 386, 2010, p. 42-

[298] Yves Poullet es Director del CRID (*Centre de Recherches Informatique et Droit*), Facultad de Derecho de Namur, Bélgica.

[299] Yves Poullet & Serge Gutwirth, "The contribution of the Article 29 Working Party to the construction of a harmonised European data protection system: an illustration of 'reflexive governance'?, en María Verónica Pérez Asinari & Pablo Palazzi (Eds) *Défis su droit à la protection de la vie privée. Challenges of privacy and data protection law*, Bruselas. Bruylant, 2008, p 570-610.

protección de datos en el tercer pilar[300]), también es cierto que el Grupo es independiente y que en más de una ocasión sus opiniones y recomendaciones han supuesto una crítica a la Comisión, por lo que también se han generado divergencias. Esto ocurrió por ejemplo con los asuntos de los PNR[301]o del Acuerdo de *Safe Harbor*, donde los acuerdos políticos alcanzados entre la Comisión y los Estados Unidos de América no se correspondían con el criterio del Grupo. Pero centrándonos en la posición de convergencia entre ambos organismos, es muy importante el reconocimiento dado por la Comisión a todo el trabajo realizado por el Grupo para contribuir a la armonización de las normativas de los distintos estados miembros.

Significativo es también el análisis sobre las alianzas con las organizaciones empresariales, sindicatos, asociaciones, organizaciones de protección al consumidor, las cuales debieran estar más presentes, pero quizás la falta de medios del Grupo hacen difícil el intercambio de opiniones con estos actores, que sería muy enriquecedor. Al menos, anualmente están invitados a las Conferencias que se organizan.

La segunda actuación destacada por *Poullet* para incrementar la visibilidad del Grupo es la ampliación de competencias, ya que por propia iniciativa, sin encargo de la Comisión, son muchos los informes y documentos elaborados en una actitud siempre proactiva del GT29, además de hacer de su trabajo una herramienta ampliamente accesible para todos, de modo que ha conseguido incrementar la accesibilidad y el conocimiento de sus actividades y estrategias.

Los dos grandes logros del Grupo de Trabajo han sido el reconocimiento del derecho fundamental a la protección de datos, consiguiendo su reconocimiento en la Carta de Derechos Fundamentales, y dotar a las empresas de herramientas para afrontar el flujo transfronterizo de datos, ideando un sistema completo y bien articulado para evaluar y asegurar el requisito de la "adecuada protección". También ha sido una

[300] Acerca del tercer pilar, ver ROBLES GARZÓN, J.A. *Nueve estudios para informar un proceso penal europeo y un código modela para potenciar la cooperación jurisdiccional iberoamericana*. Aranzadi, 2013.

[301] *Passenger Name Record* (Registro de nombres de pasajeros). Ver 221.

gran aportación el fomento de la cooperación práctica y eficaz entre todas las Autoridades de control de la Unión Europea.

La relación del Grupo de Trabajo con la Agencia de Protección de Datos Española (del que forma parte desde su creación en 1997) ha sido siempre muy cooperativa, contribuyendo al desarrollo de criterios para la unificación. Así ocurrió recientemente, en 2014, cuando ambas instituciones trabajaron conjuntamente en el documento de directrices e interpretación de la sentencia del TJUE del "derecho al olvido" dirigido a todas las Autoridades de control de la Unión para su implementación.[302]

La implicación y presencia del GT 29 en todos los estamentos de Europa en lo que a protección de datos se refiere está constatada. En los últimos tiempos ha contribuido notablemente al desarrollo del nuevo Reglamento General de Protección de Datos, emitiendo diversos dictámenes y realizando aportaciones muy útiles para la Comisión[303]. El informe más reciente, con destino al Trílogo una vez presentadas las propuestas y enmiendas por las tres instituciones (Comisión, Parlamento y Consejo), es de fecha 15 de junio de 2015[304]. En él expone su visión del Reglamento, tanto en líneas generales como entrando a valorar su posición sobre los puntos más controvertidos. Para el GT 29 el nuevo Reglamento debe ser claro, simple y eficiente, además de buscar el equilibrio que garantice los derechos individuales a la par que se preserve la innovación y la competitividad. Por otra parte, insta a los

[302] Google Spain and Inc. Vs Agencia Española de Protección de Datos y Mario Costeja González. C-131/1.2.
El documento íntegro está disponible en:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

[303] Tal y como expone la Comisión en su propuesta de Reglamento, *"Véanse, en particular, los siguientes dictámenes: sobre el «El futuro de la intimidad» (2009, WP 168); sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» (1/2010, WP 169); sobre la publicidad del comportamiento en línea (2/2010, WP 171); sobre el principio de la obligación de rendir cuentas (3/2010, WP 173); sobre la legislación aplicable (8/2010, WP 179), y sobre el consentimiento (15/2011, WP 187). A petición de la Comisión, también adoptó los tres documentos de orientación siguientes: sobre notificaciones, datos sensibles y la aplicación práctica del artículo 28, apartado 6, de la Directiva de protección de datos"*. Todos pueden consultarse en:
http://ec.europa.eu/justice/protección de datos/article-29/documentation/index_en.htm.

[304] Disponible en:
http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary.pdf.

colegisladores a dejar de lado en el nuevo Reglamento General de Protección de Datos los detalles de la implementación, entendiendo que las reglas de procedimiento deberán ser desarrolladas por el nuevo Consejo Europeo de Protección de Datos.

Los tiempos del Grupo de Trabajo del artículo 29 han tocado fin. Sus competencias serán ahora asumidas por el Consejo General de Protección de Datos, organismo de nueva creación en el nuevo Reglamento General de Protección de Datos, aumentando dichas competencias y teniendo un papel muy relevante a nivel europeo.

2.4.2 Autoridades de Control.[305]

2.4.2.1 El Supervisor Europeo de Protección de Datos (SEPD).

A.- Fundamento jurídico.

Todo el estudio hasta ahora realizado de aplicación de la normativa de protección de datos a los países de la Unión carecía de soporte normativo para la propia Administración de la Unión, ya que el reconocimiento y la aplicación del derecho ha venido siendo reconocido a los países miembros.

El Tratado de Funcionamiento de la Unión Europea (TFUE), establece en su artículo 16[306] que los actos comunitarios relativos a la protección de las personas respecto del

[305] FRA (*European Union Agency for Fundamental Rights*) *Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxemburgo, Oficina de Publicaciones de la Unión Europea (Oficina de Publicaciones), 2010.

[306] Antiguo artículo 286 del Tratado Constitutivo de la Unión Europea. DOCE de 24 de diciembre de 2002. C 325: *"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".*

tratamiento de datos personales y a la libre circulación de dichos datos serán de aplicación a las instituciones y organismos de la Unión. Asimismo, dispone la existencia de un organismo de vigilancia independiente que controle y supervise la aplicación de los actos comunitarios a las instituciones y organismos de la Comunidad. Es esta pues la base legal de creación del Supervisor Europeo de Protección de Datos.

Evidentemente, dada la supraestatalidad del ente que es la Unión Europea, en materia de protección de datos se hacía necesario un organismo de vigilancia independiente responsable de la aplicación del derecho comunitario a los organismos e instituciones de la Comunidad.

Es fundamentalmente por estas dos razones (la necesidad de una normativa de aplicación, no a los Estados -que cada uno posee la suya-, sino a los órganos e instituciones de la Unión Europea; y la necesidad igualmente de una Autoridad de control que tutelara y regulara la aplicación de dicha normativa) por las que se adoptó el Reglamento (CE) nº 45/2001 relativo a la protección de datos.

La figura del SEPD se concibió por el Parlamento y la Comisión en su redacción inicial simplemente como una Autoridad de Control[307]. Fue el Consejo Económico y Social Europeo quien, en su Dictamen sobre la Propuesta de Reglamento, recomendó que debería precisarse que la Autoridad de Control fuera Independiente[308].

El artículo 41 del Reglamento (CE) 45/2001 crea la figura del Supervisor Europeo de Protección de Datos[309], estableciendo que el nombramiento del Supervisor así como del Supervisor Adjunto correrá a cargo del Parlamento y del Consejo conjuntamente.

[307] Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre 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 sobre la libre circulación de estos datos. DOCE de 28 de diciembre de 1999. C 376 E/24. Artículo 38. 1: *"Se instituye una autoridad de control denominada «Supervisor Europeo de Protección de Datos»*.

[308] Dictamen CESE. DO C 51 de 23 de febrero de 2000. Recomendación 3.11.1: *"... debería precisarse que «se instituye una autoridad independiente de control (...)"*.

[309] Artículo 41 Reglamento 45/2001: *"1. Se instituye una autoridad de control independiente denominada «Supervisor Europeo de Protección de Datos». 2. Por lo que respecta al tratamiento de los datos personales, el Supervisor Europeo de Protección de Datos velará por que los derechos*

El procedimiento establecido para su nombramiento garantiza en gran medida la independencia, no sólo porque haya dos organismos que decidan juntos sobre su designación, sino porque dicho nombramiento será resultado de una convocatoria pública de candidaturas[310]. El procedimiento administrativo utilizado tiene apariencia de legalidad y transparencia[311]. Se publica un anuncio de puesto vacante de Supervisor Europeo de Protección de Datos y de Supervisor Adjunto, que consta de una descripción detallada del puesto de trabajo así como de los criterios de selección, los criterios de admisibilidad, la política de contratación, el procedimiento de nombramiento y el procedimiento de presentación de candidaturas[312]. Una vez presentadas las candidaturas, la Comisión elabora una lista con arreglo a su procedimiento de selección y contratación de personal [313] estableciendo un Comité de preselección que evaluará las candidaturas en función de los criterios de admisibilidad mencionados, e identifica a los candidatos cuyo perfil responda mejor a los criterios de selección para la función que van a desempeñar. A continuación hay una entrevista con el comité de preselección y quizás más entrevistas con el Comité Consultivo de nombramientos de la Comisión. Antes de celebrar esas entrevistas, los candidatos deben pasar además por un centro de evaluación dirigido por consultores externos de contratación de personal. A la vista de todo ese proceso, la Comisión

y libertades fundamentales de las personas físicas, en particular el derecho de las mismas a la intimidad, sean respetados por las instituciones y los organismos comunitarios. El Supervisor Europeo de Protección de Datos garantizará y supervisará la aplicación de las disposiciones del presente Reglamento y de cualquier otro acto comunitario relacionado con la protección de los derechos y libertades fundamentales de las personas físicas en lo que respecta al tratamiento de datos personales por parte de una institución u organismo comunitario, y asesorará a las instituciones y a los organismos comunitarios, así como a los interesados, en todas las cuestiones relacionadas con el tratamiento de datos personales. Con este fin ejercerá las funciones establecidas en el artículo 46 y las competencias que le confiere el artículo 47".

[310] Artículo 42.1 Reglamento 45/2001.

[311] Y decimos procedimiento administrativo en tanto existe un procedimiento producto de una serie de actuaciones de la Administración europea, si bien no consta descrito o reglado como tal. El derecho administrativo europeo está pendiente de ser adecuadamente desarrollado. El 15 de enero de 2013, el Parlamento Europeo aprobó su *"Resolución con recomendaciones destinadas a la Comisión sobre una Ley de Procedimiento Administrativo de la Unión Europea".*
Recomendamos la lectura de IBÁÑEZ GARCÍA, I. *Graves ausencias procedimentales en el Derecho administrativo de la Unión Europea.* Instituto de Derecho Europeo e Integración Regional (IEIR) de la Facultad de Derecho de la Universidad Complutense de Madrid, 2014.

[312] A modo de ejemplo, Publicación de un anuncio de puesto vacante de Supervisor Europeo de Protección de Datos y de Supervisor Adjunto. COM/2013/10338. DO C 219 de 31.07.2013, p 1-5. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Members Mission/Members/13-07-31_vacancies_ES.pdf.

[313] http://ec.europa.eu/civil_service/docs/official_policy_en.pdf.

elabora una lista pública con los candidatos más idóneos que remite al Parlamento Europeo y al Consejo (las cuales pueden decidir celebrar nuevas entrevistas) quienes decidirán finalmente. Posteriormente el Parlamento Europeo y el Consejo publican su Decisión por la que nombran al Supervisor y al Supervisor Adjunto[314], cuyos cargos se publican simultáneamente debiendo los candidatos haber presentado su candidatura para ambos puestos.

El primer Supervisor fue *Peter Hustinx*[315], y el primer Supervisor Adjunto Joaquín Bayo[316]. *Hustinx* fue reelegido en el segundo mandato acompañado de *Giovanni Buttarelli*[317] como Supervisor Adjunto. Este último es el actual Supervisor, siendo *Wojciech Wiewiórowski*[318] el Supervisor Adjunto.

En 2014 el procedimiento de selección, a pesar de las garantías, mostró una importante anomalía cuando en la fase de selección externa para los puestos vacantes de Supervisor y Supervisor Adjunto ningún candidato, a pesar de los brillantes currículums y la alta experiencia demostrada, fue acreditado, llegando a la absurda situación de no tener candidatos aparentemente idóneos. El Grupo de Trabajo del Artículo 29 intervino[319] solicitando una rápida solución a la Comisión alegando que el Supervisor ha de ser una persona con unas cualidades que van más allá de la mera gestión administrativa de una institución de la Unión Europea. Las plazas fueron nuevamente convocadas y finalmente cubiertas.

[314] A modo de ejemplo, la Decisión del Parlamento Europeo y del Consejo de 4.12.2014. DO L 351, de 9.12.2014.
Disponible en:
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/MembersMission/Members/14-12-04_appointingdec_ES.pdf.

[315] *Peter Hustinx* ha sido Supervisor Europeo de Protección de Datos de 2004 a 2014. Anteriormente fue Director de la Autoridad de Protección de Datos alemana y Presidente del Grupo de Trabajo del Artículo 29. También ha colaborado en el desarrollo del Convenio 108 del Consejo de Europa, en la Europol y en la Interpol.

[316] Joaquín Bayo fue Supervisor Adjunto de 2004 a 2009. También fue juez decano de Barcelona y magistrado de la Audiencia Provincial de Barcelona.

[317] *Giovanni Buttarelli* es Supervisor desde 2014. Fue Supervisor Adjunto de 2009 a 2014. Anteriormente fue Secretario General de la Autoridad de Protección de Datos italiana.

[318] *Wojciech Wiewiórowski* es Supervisor Adjunto desde 2014. Fue Inspector General de la Autoridad de Protección de Datos de Polonia y vicepresidente del Grupo de Trabajo del Artículo 29.

[319] Carta del Grupo del Artículo 29 al Presidente de la Comisión LIBE, Juan Fernando López Aguilar, de 23 de enero de 2014, al respecto del proceso de selección del Supervisor y Supervisor Adjunto: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140123_letter_on_procedure_new_edps.pdf.

B.- Funciones y competencias.

El artículo 46 del Reglamento (CE) 45/2001 determina las siguientes funciones para este organismo:

a) conocer e investigar las reclamaciones, y comunicar al interesado los resultados de sus investigaciones en un plazo razonable;
b) efectuar investigaciones por iniciativa propia o en respuesta a reclamaciones y comunicar a los interesados el resultado de sus investigaciones en un plazo razonable;
c) supervisar y asegurar la aplicación del presente Reglamento y de cualquier otro acto comunitario relacionado con la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de una institución u organismo comunitario, con excepción del Tribunal de Justicia de las Comunidades Europeas cuando actúe en el ejercicio de sus funciones jurisdiccionales;
d) asesorar a todas las instituciones y organismos comunitarios, tanto a iniciativa propia como en respuesta a una consulta, sobre todos los asuntos relacionados con el tratamiento de datos personales, especialmente antes de la elaboración por dichas instituciones y organismos de normas internas sobre la protección de los derechos y libertades fundamentales en relación con el tratamiento de datos personales;
e) hacer un seguimiento de los hechos nuevos de interés, en la medida en que tengan repercusiones sobre la protección de datos personales, en particular de la evolución de las tecnologías de la información y la comunicación;
f) colaborar con las Autoridades de control nacionales a que se refiere el artículo 28 de la Directiva 95/46/CE de los países a los que se aplica dicha Directiva en la medida necesaria para el ejercicio de sus deberes respectivos, en particular intercambiando toda información útil, instando a dicha autoridad u organismo a ejercer sus poderes o respondiendo a una solicitud de dicha autoridad u organismo; colaborar asimismo con los organismos de control de

la protección de datos establecidos en virtud del Título VI del Tratado de la Unión Europea, en particular con vistas a mejorar la coherencia en la aplicación de las normas y procedimientos de cuyo respeto estén respectivamente encargados;

g) participar en las actividades del «Grupo de trabajo sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales» creado en virtud del artículo 29 de la Directiva 95/46/CE;
h) determinar, motivar y hacer públicas las excepciones, garantías, autorizaciones y condiciones mencionadas en la letra b) del apartado 2 y en los apartados 4, 5 y 6 del artículo 10 (en relación con el tratamiento de datos de categorías especiales), en el apartado 2 del artículo 12 (sobre la excepción al deber de información cuando los datos no han sido recabados del interesado), en el artículo 19 (sobre las excepciones a decisiones individuales automatizadas) y en el apartado 2 del artículo 37 (sobre el tratamiento de datos de tráfico);
i) mantener un registro de los tratamientos que se le notifiquen en virtud del apartado 2 del artículo 27 (controles previos) y hayan sido registrados conforme al apartado 5 del artículo 27, así como facilitar los medios de acceso a los registros que lleven los responsables de la protección de datos con arreglo al artículo 26;
j) efectuar una comprobación previa de los tratamientos que se le notifiquen;
k) adoptar su Reglamento interno.

El artículo 47 del Reglamento (CE) 45/2001 establece las competencias del Supervisor Europeo de Protección de Datos:

a) asesorar a las personas interesadas en el ejercicio de sus derechos;
b) acudir al responsable del tratamiento en caso de presunta infracción de las disposiciones que rigen el tratamiento de los datos personales y, en su caso, formular propuestas encaminadas a corregir dicha infracción y mejorar la protección de las personas interesadas;

c) ordenar que se atiendan las solicitudes para ejercer determinados derechos respecto de los datos, cuando se hayan denegado dichas solicitudes incumpliendo los artículos 13 a 19;
d) dirigir una advertencia o amonestación al responsable del tratamiento;
e) ordenar la rectificación, bloqueo, supresión o destrucción de todos los datos que se hayan tratado incumpliendo las disposiciones que rigen el tratamiento de datos personales y la notificación de dichas medidas a aquellos terceros a quienes se hayan comunicado los datos;
f) imponer una prohibición temporal o definitiva del tratamiento;
g) someter un asunto a la institución u organismo comunitario de que se trate y, en su caso, al Parlamento Europeo, al Consejo y a la Comisión;
h) someter un asunto al Tribunal de Justicia de las Comunidades Europeas en las condiciones previstas en el Tratado, e
i) intervenir en los asuntos presentados ante el Tribunal de Justicia de las Comunidades Europeas.

El Supervisor Europeo de Protección de Datos estará habilitado para:

a) obtener de cualquier responsable del tratamiento o de una institución o un organismo comunitario el acceso a todos los datos personales y a toda la información necesaria para efectuar sus investigaciones, y
b) obtener el acceso a todos los locales en los que un responsable del tratamiento o una institución u organismo comunitario realice sus actividades, cuando haya motivo razonable para suponer que en ellos se ejerce una actividad contemplada en el Reglamento.

A pesar de las funciones y competencias determinadas en el Reglamento (CE) 45/2001, el devenir y la evolución del propio organismo ha ido dotándolo de un contenido más ajustado a la realidad. Así, en la publicación del anuncio del puesto vacante de los Supervisores de 2013[320], describe las tareas incluyendo algunas que no están expresamente recogidas en el Reglamento (CE) 45/2001, tales como la

[320] Ver 312.

cooperación con los organismos supervisores de protección de datos creados en el contexto de la cooperación policial y judicial en la Unión; el control de la transferencia de datos a destinatarios distintos de las instituciones, organismos, agencias y oficinas de la Unión Europea, que no estén sujetos a la Directiva 95/46/CE; la actuación como Autoridad de control para el sistema "*Eurodac*"[321] o la actuación también como Autoridad de control de protección de datos en el Sistema de Información de Visados (VIS) y el Sistema de Información de *Schengen* de segunda generación (SIS II), el Sistema de Información del Mercado Interior (IMI), *Frontex,* el Sistema de Información Aduanero (SIA) y otras bases de datos específicas en el marco de la legislación aduanera.

También se establece en la descripción del puesto de trabajo del Supervisor que podrá estar llamado a asumir nuevos cometidos y competencias cuando entre en vigor el nuevo marco jurídico de la UE sobre protección de datos. Efectivamente, el próximo Reglamento General de Protección de Datos asigna nuevas competencias para el SEPD que incrementarán notablemente su trabajo, tales como ser miembro del nuevo Consejo Europeo de Protección de Datos (CEPD)[322] y asumir la Secretaría de éste último[323]. Si bien el CEPD sustituye al Grupo de Trabajo del artículo 29, al cual ya pertenecía el Supervisor Europeo de Protección de Datos, no es menos cierto que las competencias del Consejo son mucho mayores que las del Grupo de Trabajo, por lo que la actividad del Supervisor se verá ampliada en este punto, teniendo incluso con carácter permanente el cargo de uno de los dos Vicepresidentes (cuando no fuera Presidente)[324]. Pero sin lugar a dudas, será la llevanza de la Secretaría la que

[321] Sistema que asiste a los estados miembros a la hora de determinar quién es competente en las solicitudes de asilo y de facilitar la aplicación del Convenio de Dublín.

[322] Artículo 64.2 Propuesta de Reglamento General de Protección de Datos, versión Comisión: *"El Consejo Europeo de Protección de Datos estará compuesto por el director de una autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de Datos".*

[323] Artículo 71 Propuesta de Reglamento General de Protección de Datos, versión Comisión: *"El Consejo Europeo de Protección de Datos contará con una secretaría. El Supervisor Europeo de Protección de Datos se hará cargo de dicha secretaría".*

[324] Artículo 64.2 Propuesta de Reglamento General de Protección de Datos: *"El Consejo Europeo de Protección de Datos estará compuesto por el director de una autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de Datos".*
Artículo 69.1 Propuesta de Reglamento General de Protección de Datos, versión Comisión. *"El Consejo Europeo de Protección de Datos elegirá de entre sus miembros un presidente y dos vicepresidentes. Uno de los vicepresidentes será el Supervisor Europeo de Protección de Datos, salvo que haya sido elegido presidente".*

ocupará más recursos del Supervisor. La Secretaría será la encargada de prestar apoyo analítico, administrativo y logístico al Consejo Europeo de Protección de Datos, bajo la dirección del Presidente, concretándose su responsabilidad en las siguientes tareas[325]:

- los asuntos corrientes del Consejo Europeo de Protección de Datos;
- la comunicación entre los miembros del Consejo Europeo de Protección de Datos, su presidente y la Comisión, así como de la comunicación con otras instituciones y con el público;
- la utilización de medios electrónicos para la comunicación interna y externa;
- la traducción de la información pertinente;
- la preparación y el seguimiento de las reuniones del Consejo Europeo de Protección de Datos y
- la preparación, redacción y publicación de dictámenes y otros textos adoptados por el Consejo Europeo de Protección de Datos.

El nuevo instrumento normativo en protección de datos para la Unión Europea detalla numerosas competencias para las Autoridades de control nacionales, si bien ninguna de ellas afecta al Supervisor Europeo de Protección de Datos, ya que deja fuera de su ámbito de aplicación a las instituciones y organismos de la Unión Europea[326] (al menos en la propuesta de la Comisión y en la del Consejo, que no en la del Parlamento), cuestión difícil de entender y que desde nuestro punto de vista hace que la armonización (que en su totalidad será casi imposible) quede a medio camino. Por ello entendemos que se hace imprescindible, una vez finalicen las negociaciones y se publique un texto definitivo, si éste no incluye finalmente en su ámbito de aplicación a la administración europea, se proceda a la modificación del Reglamento (CE) 45/2001 de modo que los derechos de los ciudadanos y las obligaciones de los responsables y encargados del tratamiento sean idénticas en todas

[325] Artículo 71. 2 y 3 Propuesta de Reglamento General de Protección de Datos, versión Comisión.
[326] Artículo 2.2.b Propuesta de Reglamento General de Protección de Datos, versión Comisión: *"El presente Reglamento no se aplica al tratamiento de datos personales: b) por parte de las instituciones, órganos u organismos de la Unión".*

las instituciones y organismos de Europa, tanto en el fondo como en la forma, debiendo aprovechar también esa modificación, si se produjese, para actualizar legislativamente las funciones y competencias del Supervisor Europeo de Protección de Datos.

C.- Áreas de trabajo.

Todas las funciones desarrolladas por el Supervisor que acabamos de describir se concentran en tres ámbitos de actuación: supervisión, asesoramiento y cooperación[327]. Los inicios del Supervisor, de la mano de *Peter Hustinx* y Joaquín Bayo, son muy recientes, pues comenzó su andadura en 2004, con una oficina con cuatro personas y teniendo que construir una nueva institución[328], para lo que no dudaron en formarse con quienes eran los oficiales de protección de datos de las principales instituciones de la Unión Europea, intercambiando información y experiencia.

1.- **El área de Supervisión** es la principal razón de ser del SEPD. Esta tarea de supervisar el tratamiento de datos de carácter personal en las instituciones y organismos de la Unión Europea se lleva a cabo de varias formas:

- A través de la comprobación con carácter previo *(prior check*) de tratamientos que presentan riesgos específicos y que le son notificados al SEPD por los Oficiales de protección de datos de cada organismo (DPO). En la mayoría de los casos, ello supone una serie de recomendaciones que hace el SEPD y que debe implementar el organismo en cuestión para garantizar el cumplimiento de las normas[329].

[327] Para mayor información consultar la web del SEPD: https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS

[328] Al respecto BAYO DELGADO, J. "Setting up a new European Authority", en Hielke Hijmans and Herke Kranenborg (Eds) *Data Protection Anno 2014: How to restore Trust?,* Cambridge. Intersentia, 2014, p 45-48.

[329] LOUVEAUX, SOPHIE. "Ten Years of supervisión of the EU Institutions and Bodies", en Hielke Hijmans and Herke Kranenborg (Eds) *Data Protection Anno 2014: How to restore Trust?*. Cambridge. Intersentia, 2014, p. 256. "El trabajo de control previo ha proporcionado una

- Gestionando las quejas de los ciudadanos que entienden que sus datos no han sido correctamente tratados, así como de los propios miembros del personal de la Unión Europea.
- Emitiendo dictámenes sobre medidas a adoptar por instituciones y organismos en la UE.
- Llevando a cabo inspecciones e investigaciones in situ, tanto por iniciativa propia como previa denuncia.
- Manteniendo relaciones constantes con los DPO de todos los organismos europeos, participando en reuniones periódicas. Juntos forman una red de la que también forma parte el SEPD[330]. Se realiza también un seguimiento del cumplimiento por las instituciones de esta figura.[331]
- Publicando directrices temáticas sobre asuntos cruciales para ayudar en su cumplimiento, tales como conflicto de intereses[332]; los derechos de las personas[333] o contratación pública, subvenciones y expertos externos[334],

oportunidad para establecer un diálogo preventivo con las instituciones de la UE en forma de reuniones o consultas públicas con el objetivo de promover una cultura positiva y proactiva en relación con la protección de datos dentro de la administración de la UE. Esta tarea también permite al SEPD hacerse una idea de las actividades de las instituciones de la UE, y le ayuda a identificar las cuestiones clave de protección de datos así como el desarrollo de la propia jurisprudencia del SEPD. Por último, la experiencia adquirida en la aplicación del Reglamento también permitió al SEPD ganar conocimientos y proporcionar directrices temáticas a las instituciones y organismos".

[330] Esta red hizo público un valioso documento para los DPO sobre los Estandar Profesionales de los DPO de las instituciones y organismos de la Unión Europea bajo el Reglamento 45/2001. Disponible en: http://ec.europa.eu/dataprotectionofficer/docs/dpo_standards_en.pdf.

[331] Documento acerca del rol del DPO en cumplimiento del artículo 24 del Reglamento 45/2001: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PositionP/05-11-28_DPO_paper_EN.pdf.
Documento relativo al cumplimiento por los DPO de las instituciones de la UE: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Inquiries/2012/2012-12-17_DPO_Status_web_EN.pdf.

[332] Disponible en: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/14-12-08_CoI_Guidelines_EN.pdf.

[333] Disponible en: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/14-02-25_GL_DS_rights_EN.pdf

[334] Disponible en: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/13-06-25_Procurement_EN.pdf

tareas, obligaciones y competencias del responsable de protección de datos[335] o los datos de salud en el trabajo[336].

- Llevando el control y la supervisión del Eurodac[337].

2.- **El área de Asesoramiento** en el Supervisor Europeo de Protección de Datos ha tenido un crecimiento exponencial. La tarea de asesorar en todas las propuestas legislativas que afecten a la protección de datos personales ha supuesto en los últimos tiempos una actividad de gran alcance, ya que cada vez son más las áreas legislativas (por no decir casi todas) que afectan a esta materia. Si a esto le sumamos que también ha de asesorar en los instrumentos conocidos como *soft law*[338] podemos apreciar que su trabajo es voluminoso y requiere de un gran despliegue profesional. Existe además un asesoramiento previo (que podríamos denominar confidencial) a las distintas Direcciones Generales de la Comisión en materias que puedan verse afectadas por la protección de datos, y que pueden ser una medida, una propuesta legislativa o un documento público, y ello independientemente de la opinión pública que emite posteriormente el SEPD. Es la denominada "consulta informal" que recoge el artículo 27 de su Reglamento interno[339]. También asesoran a la Comisión a través

[335] Disponible en: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-07-29_Guidelines_DPO_tasks_EN.pdf

[336] Disponible en: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/09-09-28_Guidelines_Healthdata_atwork_EN.pdf

[337] El Sistema Eurodac es una base informatizada de datos dactiloscópicos que permite a los países de la Unión Europea (UE) ayudar a identificar a los solicitantes de asilo y a las personas interceptadas en relación con el cruce irregular de las fronteras exteriores de la Unión. Comparando sus huellas, los países de la UE pueden comprobar si un solicitante de asilo o un extranjero presente ilegalmente en su territorio ya ha solicitado asilo en otro país de la UE, o si un solicitante de asilo ha entrado irregularmente en el territorio de la Unión. Además de las huellas, los datos transmitidos por los países de la UE incluyen el país de la UE de origen; el sexo de la persona; el lugar y fecha de la solicitud de asilo o la interceptación de la persona; el número de referencia; la fecha de toma de impresiones dactilares y la fecha de transmisión de datos a la unidad central.

[338] El *soft law* es el conjunto de instrumentos que careciendo de rango normativo han sido creados por instituciones con poder legislativo y adquieren relevancia jurídica. A modo de ejemplo, las decisiones o recomendaciones.

[339] Decisión del Supervisor Europeo de Protección de Datos de 17.01.2012 relativa a la adopción del Reglamento interno. DO L 273, p.45.

de los Comentarios sobre las Comunicaciones que ésta presenta en el seguimiento de determinadas políticas[340].

Además de estos cometidos, es competencia del área de Asesoramiento el seguimiento de las nuevas tecnologías[341], para lo que deberá identificar las tendencias emergentes que puedan tener impacto potencial en la protección de datos, estableciendo contactos con las partes interesadas, y concienciando y asesorando sobre todas aquellas cuestiones en esta materia que puedan afectarles, promoviendo los principios de intimidad mediante el diseño y privacidad por defecto y, en su caso, adaptar las metodologías de supervisión a los avances tecnológicos[342]

Por último, el Supervisor dando asesoramiento, interviene en procedimientos judiciales[343] ante el Tribunal de Justicia de la Unión Europea, el Tribunal General y el Tribunal de la Función Pública. Puede hacerlo actuando contra las instituciones, como parte en los procedimientos en que se recurran sus Decisiones, o bien simplemente ante el Tribunal de Justicia de la Unión Europea como experto a fin de dar una opinión sobre la materia, ya sea por deseo expreso de la propia SEPD (previa autorización) o bien porque el Tribunal le invite a hacerlo. Su intervención ha sido muy importante en asuntos recientes como el caso *Schrems* vs Comisión[344] o el caso Comisión vs Hungría[345].

Para llevar a cabo estos trabajos, el SEPD planifica anualmente sobre las propuestas legislativas de la Comisión que probablemente tendrán más impacto y requerirán de

[340] A modo de ejemplo, Comentarios sobre Estrategia de Red de Agencias de Medicamentos de la UE para 2020. Disponible en: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2015/15-06-19_EUMA_Network_Strategy_EN.pdf.

[341] Opinión 1/2015 sobre sanidad móvil: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-05-21_Mhealth_EN.pdf.

[342] Artículo 38 Decisión del Supervisor Europeo de Protección de Datos de 17.01.2012 relativa a la adopción del Reglamento interno. DO L 273, p.47.

[343] Artículo 41 Decisión del Supervisor Europeo de Protección de Datos de 17.01.2012 relativa a la adopción del Reglamento interno. DO L 273, p.48.

[344] Caso C-362/14, *Schrems vs Data Protection Commissioner* https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2015/15-03-24_EDPS_Pleading_Schrems_vs_Data_Commissioner_EN.pdf

[345] Caso C.288/12, Comisión vs Hungría https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2013/13-10-15_Pleading_EC-Hungary_EN.pdf

una mayor atención por su parte, y también elabora Dictámenes dirigidos a orientar a quienes forman parte del debate legislativo en las nuevas propuestas. En este sentido, la actividad del SEPD respecto del nuevo Reglamento General de Protección de Datos ha sido proactiva e incesante. Además de las opiniones realizadas a través del GT 29, son varias las publicadas desde el propio Supervisor. Destacamos por su proximidad en el tiempo el Dictamen 3/2015 (Recomendaciones del SEPD sobre las opciones de la UE en cuanto a la reforma de la protección de datos)[346] publicado conjuntamente con el cuadro comparativo a cuatro columnas que incluye los textos de la Comisión, del Parlamento, del Consejo y la propuesta del SEPD[347]; así como la Adenda al mismo hecha pública el 9 de octubre de 2015 donde reitera la necesidad de un texto flexible, con un enfoque ético y bajo una redacción clara y concisa[348]; todo ello con la finalidad de ayudar en su difícil tarea a quienes participan en el trílogo[349], dando su visión de cuál debería ser el texto idóneo[350]y cuáles deberían de ser los principios sobre los que se construya el texto.

3.- **El área de Cooperación** es el tercer sector del trabajo del Supervisor, cuyo principal objetivo siempre es conseguir la armonización de criterios en interpretación de la Directiva. Su labor se concreta en varias parcelas:

[346] Dictamen 3/2015 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_ES.pdf

[347] Cuadro comparativo. Disponible en: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_Annex_EN.pdf

[348] Addenda.- https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-10-09_GDPR_with_addendum_EN.pdf

[349] Se puede consultar en un cuadro comparativo con las otras tres propuestas en: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_Annex_EN.pdf

[350] Dictamen 3/2015. Ver: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_ES.pdf.

a) Con las Autoridades nacionales de control en materia de protección de datos a través del intercambio de información, desarrollo y mantenimiento del contacto con el personal[351].
b) La cooperación a través del Grupo de Trabajo del Artículo 29[352]. Su opinión representa la opinión de la Unión y contribuye activamente a las discusiones y elaboración de dictámenes, cuya finalidad es contribuir a la interpretación de la Directiva 95/46/CE y prestar asesoramiento a la Comisión Europea, dictámenes a los que hemos hecho varias referencias a lo largo de este trabajo.
c) También participa en el tercer pilar de la Unión Europea para asegurar una buena gestión de la protección de datos en la cooperación judicial y policial en materia penal, así como en el Grupo de Trabajo sobre Policía y Justicia, creado por la Conferencia Europea.
d) Uno de los cometidos de mayor relevancia en materia de cooperación es su participación en el Eurodac, que necesita de un enfoque y coordinación por parte del SEPD, ya que es una base de datos formada por una unidad central (sujeta a la normativa de protección de datos para los órganos e instituciones comunitarias), y varias unidades nacionales (que se regirán por la normativa nacional).
e) El SEPD organiza dos conferencias anuales: una en primavera, la Conferencia Europea -que agrupa a representantes de los Estados miembros así como del Consejo de Europa-; y otra en otoño, la Conferencia Internacional -que reúne a expertos en protección de datos, tanto de sectores privados como públicos-.
f) También ha contribuido a la organización de talleres (*workshop*) colaborando con organizaciones internacionales[353].

[351] Artículo 46 f) inciso i) Reglamento 45/2001.
[352] Artículo 46 g) Reglamento 45/2001.
[353] "*Workshop on data protection as part of good governance in international organizations*".Geneve, septiembre 2005. Organizada por el SEPD, el Consejo de Europa y la OCDE.
"*The role of an internal and independent data protection officer*". Munich, marzo 2007. Organizada por la Oficina de Patentes Europea.
"*How to ensure accountability in personal data management*". Florencia, mayo 2007. Organizada por European University Institute of Florence.

D.- El Supervisor y el Supervisor Adjunto. Un caso de bicefalia.

Cuestión jurídicamente interesante es la figura del Supervisor y del Supervisor Adjunto.

Del texto del artículo 42 del Reglamento (CE) 45/2001 así como de los artículos 1 y 2 de la Decisión relativa al estatuto y a las condiciones generales de ejercicio de las funciones del Supervisor[354] parece deducirse la existencia de una relación jerárquica entre ambos, donde el Supervisor estuviera en la parte más alta, además de ser la imagen pública de la Institución. Dice el artículo 42 del Reglamento: *"Se nombrará a un Supervisor Adjunto de conformidad con el mismo procedimiento y por un periodo de igual duración. Asistirá al Supervisor en todas sus funciones y le sustituirá en caso de ausencia"*. Dicen los artículos 1 y 2 de la Decisión, respecto de la retribución de ambos: *"el Supervisor Europeo de Protección de Datos queda asimilado a los jueces del Tribunal de Justicia de las Comunidades Europeas"*[355], mientras que el Supervisor Adjunto lo es *"al Secretario del Tribunal de Justicia de las Comunidades Europeas"*[356].

Sin embargo la realidad es bien distinta, pues ambos cargos comparten funciones y poder. La designación de ambos –que se lleva a cabo en un .proceso público y transparente- les exige iguales requisitos para su nombramiento[357], y les asigna las mismas funciones. El artículo 42.8 del Reglamento (CE) 45/2001 también reconoce esta equivalencia cuando dice *"Los apartados 2 a 7 serán aplicables al Supervisor*

"*Data protection within international organisations*".Bruselas, noviembre 2012. Organizada por la World Customs Organisation (WCO).
Está previsto un quinto workshop en Genova, el febrero de 2016, organizado por el *International Committee of the Red Cross* y el SEPD.

[354] Decisión 1247/2002/CE del Parlamento Europeo, del Consejo y de la Comisión, de 1 de julio de 2002, relativa al estatuto y a las condiciones generales de ejercicio de las funciones de Supervisor Europeo de Protección de Datos. DO L 183, p. 1 y 2, de 12.07.2002.

[355] Artículo 1 Decisión 1247/2002/CE.

[356] Artículo 2 Decisión 1247/00/CE.

[357] Artículo 42.1 del Reglamento 45/2001.

Adjunto". Pero es más, el Reglamento interno del SEPD[358], en su artículo 2 recoge la definición de "el supervisor" como "*salvo disposición en contrario, las personas que ejercen las funciones de Supervisor Europeo de Protección de Datos y de Supervisor adjunto".* En el mismo sentido, el artículo 4 de dicho Reglamento interno describe las funciones de ambos en plena equivalencia: *"Funciones del supervisor y del supervisor adjunto.- 1. El supervisor y el supervisor adjunto serán, como miembros de la institución, responsables de la adopción de estrategias, políticas y decisiones, y trabajarán juntos en el ejercicio de las funciones mencionadas en el artículo 1. El supervisor adjunto desempeñará dichas funciones, en caso de ausencia o impedimento del Supervisor y viceversa. 2. El supervisor y el supervisor adjunto tendrán como objetivo llegar a un consenso sobre las estrategias y las políticas generales y otras cuestiones importantes, incluidas las relacionadas con la secretaría. El supervisor adoptará una decisión cuando no sea posible el consenso y la cuestión sea urgente. 3. El supervisor, actuando en estrecha colaboración con el supervisor adjunto, establecerá una división del trabajo entre ellos, que incluirá cuál de ellos será el responsable principal de la elaboración, adopción y seguimiento de las decisiones y de la delegación de funciones al supervisor adjunto, en su caso"*. A mayor abundamiento, el organigrama de la organización los sitúa en idéntica posición[359].

Estamos pues ante un caso de bicefalia del Supervisor, donde ambos cargos, Supervisor y Supervisor Adjunto, comparten estatus y funciones, compensando poder y haciendo del consenso una estrategia para la gobernanza.

2.4.2.2 La Autoridad Común de Control de la Europol.

El marco legislativo europeo de referencia en protección de datos, la Directiva 95/46/CE y el Reglamento (CE) 45/2001, excepcionan de su ámbito de aplicación el

[358] Decisión del Supervisor Europeo de Protección de Datos de 17.12.2012 relativa a la adopción del Reglamento interno. DO L 273, p. 41 a 50, de 15.10.2013.

[359] Disponible en: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/HR/EDPS_organigram_EN.pdf.

tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal[360].

Para colaborar en estos campos y tener una adecuada protección en el tratamiento de estos datos, se creó en 1995 la Oficina de Policía Europea mediante el Convenio basado en el artículo K.3 del Tratado de la Unión Europea por el que se establece una Oficina Europea de Policía (Convenio Europol)[361], encargada de mejorar la cooperación entre las autoridades policiales y los servicios de seguridad de los Estados miembros. El 1 de enero de 2010, al aprobarse la Decisión 2009/371/JAI del Consejo[362] que sustituía al Convenio, Europol se convirtió en Agencia de la UE de pleno derecho, dotada de un nuevo marco jurídico y un mandato más amplio[363].

Los órganos de Europol son: un Consejo de Administración[364], con representantes de los Estados miembros y de la Comisión Europea y que decide sobre las líneas de actuación de la institución; y un Director[365], quien ostenta la representación de la Agencia y se ocupa de la gestión operativa de la misma, incluyendo la organización de las diferentes unidades de investigación. La sede central, ubicada en La Haya, también cuenta con oficinas de enlace de todos los Estados miembros así como de otros Estados u organizaciones con las que Europol mantiene acuerdos de colaboración. Finalmente, cada Estado miembro mantiene una unidad nacional de Europol que se encarga de gobernar los flujos de comunicación entre los Estados miembros y la sede central. El Consejo de Administración nombra, a propuesta del Director, un responsable de la protección de datos, que es un miembro del personal.

[360] Artículo 3 Directiva 95/46/CE, de 24 de octubre, 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 (DOCE L 281, de 23 de noviembre).
[361] Convenio basado en el artículo K.3 del Tratado de la Unión Europea por el que se crea una oficina europea de policía (Convenio Europol), hecho en Bruselas el 26 de julio de 1995. BOE 232, de 28 de septiembre de 1998.
[362] Decisión del Consejo de 6 de abril de 2009 (2009/371/JAI). DOUE de 15 de mayo de 2009. L 121.
[363] Sobre Europol, DREWER, D. y ELLERMANN, J., *Europol's data protection framework as an asset in the fight against cybercrime*, Foro ERA, Vol. 13, núm. 3, 2013, p. 381–395.
[364] Artículo 37 Decisión 2009/371/JAI.
[365] Artículo 38 Decisión 2009/371/JAI.

En el desempeño de sus funciones, dicho responsable actuará con independencia y son muchas las funciones que se le designan.[366]

Parte muy importante de la actuación de Europol consiste, por un lado, en facilitar la transmisión de información entre los servicios nacionales y, por otro, en proporcionar análisis de la delincuencia a estos servicios. Europol sólo puede tratar datos personales en el desempeño de sus funciones. En el mismo sentido, el acceso a los datos de carácter personal tratados por la Agencia está limitado a las autoridades competentes de los Estados miembros que el Estado cedente autorice.[367]

La protección y seguridad de los datos está regulada en el Capítulo V de la Decisión 2009/371/JAI. Tiene en cuenta los principios del Convenio 108 del Consejo de Europa y la Recomendación nº R (87) 15, de 17 de septiembre de 1987, del Comité de Ministros del Consejo de Europa. Europol tiene que respetar dichos principios en el tratamiento de datos personales, incluidos los datos automatizados y no automatizados que obren en su poder en forma de ficheros, en especial cualquier conjunto estructurado de datos personales accesible según criterios determinados[368].

Asímismo, la Decisión recoge quién es el responsable por el tratamiento de datos (el Estado que transmite y Europol)[369], los derechos de los interesados (acceso[370] y rectificación y supresión de datos[371]). Establece una serie de medidas técnicas y

[366] Artículo 28 Decisión 2009/371/JAI: "El responsable de la protección de datos tendrá, en particular, las funciones siguientes: a) garantizar, de manera independiente, la legalidad y el cumplimiento de las disposiciones de la presente decisión en lo que respecta al tratamiento de datos personales, incluido el tratamiento de datos personales relativos al personal de Europol; b) asegurarse de que se lleve un registro escrito de la transmisión y recepción de datos personales, en cumplimiento de lo dispuesto en la presente Decisión; c) garantizar que las personas a que se refieran los datos sean informadas, cuando así lo soliciten, de sus derechos con arreglo a la presente Decisión; d) cooperar con el personal de Europol responsable de los procedimientos, la formación y el asesoramiento en materia de tratamiento de datos; e) cooperar con la autoridad común de control; f) elaborar un informe anual y transmitirlo al consejo de administración y a la autoridad común de control.

[367] Artículo 24.1 Decisión 2009/371/JAI.

[368] Artículo 27 Decisión 2009/371/JAI.

[369] Artículo 29 Decisión 2009/371/JAI.

[370] Artículo 30 Decisión 2009/371/JAI.

[371] Artículo 31 Decisión 2009/371/JAI.

organizativas necesarias de ejecutar para la seguridad de los datos[372], además de recoger el principio de confidencialidad[373]

De acuerdo a la Decisión Europol, los afectados tienen el derecho a solicitar el acceso a los datos personales que le conciernan, así como a la modificación o cancelación los mismos en caso de que sean incorrectos.

La Decisión 2009/371 establece en su artículo 33 la obligatoriedad de tener una Autoridad Nacional de Control *"cuya tarea consistirá en vigilar, de manera independiente y con arreglo a la legislación nacional, la licitud de la introducción, la consulta de datos y todo tipo de transmisión de datos personales a Europol por parte del Estado miembro de que se trate, y en verificar que no se vulneran los derechos de las personas a las que se refieren los datos".* En España, dichas funciones son asumidas por la Agencia Española de Protección de Datos.

Y en lo que al desarrollo de este apartado se refiere, resulta especialmente relevante la creación de una Autoridad Común de Control de Europol, desarrollada en el artículo 34 de la Decisión 2009/371, cuyo cometido es vigilar la actividad de Europol para *"garantizar que el almacenamiento, el tratamiento y la utilización de los datos de que dispongan los servicios de Europol no vulneren los derechos de las personas",* y "*controlará además la licitud de la transmisión de datos que procedan de Europol*". Su Reglamento interno establece cuáles serán las funciones de este organismo[374]. La Autoridad Común de Control está constituida por un máximo de dos miembros de cada una de las autoridades nacionales de control independientes,

[372] Artículo 35 Decisión 2009/371/JAI.
[373] Artículo 40 Decisión 2009/371/JAI.
[374] Acto Núm. 29/2009 de la Autoridad Común de Control de Europol de 22 de junio de 2009 por el que establece su Reglamento interno. BO C 45, p 2-13).
Artículo 2: "1. La Autoridad Común de Control tendrá por función examinar y vigilar, de acuerdo con la Decisión de Europol, la actividad de Europol a fin de garantizar que el almacenamiento, el tratamiento y la utilización de los datos de que disponga Europol no vulneran los derechos de las personas. La Autoridad Común de Control controlará además la licitud de la transmisión de los datos que procedan de Europol (frases primera y segunda del apartado 1 del artículo 34 de la Decisión de Europol)".

con las aptitudes necesarias, y nombrados por cada Estado miembro por períodos de cinco años. El Presidente es uno de sus miembros.

En el ejercicio de sus funciones, los miembros de la Autoridad Común de Control no reciben instrucciones de ninguna autoridad.

La Autoridad Común de Control se ocupa de garantizar qué tratamiento de los datos de carácter personal por parte de Europol se realiza conforme a la legalidad. Para ello, se ocupa de revisar sus actividades así como la atención a reclamaciones de los afectos en relación con el ejercicio de los derechos de acceso, rectificación y cancelación de sus datos de carácter personal. *"Será competente para analizar las dificultades de aplicación e interpretación que pudiera plantear la actividad de Europol en relación con el tratamiento y la utilización de datos personales, para estudiar los posibles problemas en relación con el control independiente efectuado por las autoridades nacionales de control de los Estados miembros o con el ejercicio del derecho de acceso y para elaborar propuestas armonizadas con miras a hallar soluciones comunes a los problemas existentes".*

"Para el cumplimiento de sus funciones y para contribuir a mejorar la coherencia de la aplicación de las normas y procedimientos del tratamiento de datos, la autoridad común de control cooperará en la medida necesaria con otras autoridades de supervisión".[375]

También elaborará informes de actividad a intervalos regulares. Estos informes se transmitirán al Parlamento Europeo y al Consejo, decidiendo la Autoridad Común de Control si procede o no publicar su informe de actividad y, en caso afirmativo, decidirá las condiciones de dicha publicación. Son muchos los informes que esta Autoridad de Control emite[376].

[375] Artículo 34 Decisión 2009/371/JAI.

[376] Los más recientes son:

- "Report on the data protection perspective of the processing of data on victims of trafficking in human beings": http://www.europoljsb.europa.eu/media/277384/on%2012%20october%202015.pdf.
- "Report on the Europol´s implementation of the TFTP Agreement":

En su estructura existe un Comité integrado por un representante cualificado de cada Estado miembro, cada uno de los cuales tendrá derecho a un voto, y que se encargará de examinar los recursos contemplados en el artículo 32, para lo cual podrá utilizar todos los medios pertinentes. Si las partes lo solicitan, comparecerán ante el Comité, asistidas por sus asesores si lo desean. Las decisiones adoptadas en este marco serán definitivas para todas las partes afectadas.

En marzo de 2013 la Comisión Europea presentó una propuesta de Reglamento[377] con el fin de dar cumplimiento a lo establecido en el Tratado de Lisboa[378], por lo que sus disposiciones han pasado a formar parte del Tratado de Funcionamiento de la Unión Europea (Título V, Espacio de libertad, seguridad y justicia). El desarrollo normativo se está llevando a cabo por el procedimiento legislativo ordinario, por el Parlamento Europeo y por el Consejo. Tanto la Autoridad Común de Control[379] como el Supervisor Europeo de Protección de Datos han presentado opiniones en relación con el proyecto centradas en las disposiciones específicas sobre protección de datos.

http://www.europoljsb.europa.eu/media/276578/report%20on%20the%20europol.pdf

- "Data Protection Inspection Report September 2014": http://www.europoljsb.europa.eu/media/267640/14-41%20final%20data%20inspection%20report%20september%202014-%20v07.pdf.

[377] Propuesta de Reglamento del Parlamento Europeo y del Consejo 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 y 2005/681/JAI. Bruselas, 27.3.2013 COM(2013).
Para mayor información:
http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0173_/com_com(2013)0173_es.pdf

[378] Artículo 88 Tratado de Lisboa, por el que se modifican el Tratado de la Unión Europea y el Tratado Constitutivo de la Comunidad Europea.

[379] Para consultar el último informe de la Autoridad Común de Control de la Europol sobre el nuevo Reglamento ver el "Tercer dictamen de la Autoridad Común de Control de Europol. Dictamen 14/39 en relación con la Orientación General aprobada por el Consejo de la Unión Europea para un Reglamento del Parlamento Europeo y del Consejo sobre la Agencia de la Unión Europea para la cooperación y la formación en funciones coercitivas (Europol)":
http://www.europoljsb.europa.eu/media/266424/op%2014-39%20third%20jsb%20op.%20for%20ep%20&%20council%20reg.%20on%20europol.es.pdf.

2.4.2.3 La Autoridad Común de Control de Schengen.

El Acuerdo de *Schengen*, firmado el 14 de junio de 1985 entre Alemania, Bélgica, Francia, Luxemburgo y los Países Bajos, y su Convenio de Aplicación, de 19 de junio de 1990[380], crea un espacio libre en varios países de Europa en el que se suprimen las fronteras entre ellos, quedando únicamente las fronteras exteriores con el resto de países. No entró en vigor hasta 1995.

El Acuerdo y el Convenio así como las normas y acuerdos conexos conforman el «acervo de *Schengen*», el cual desde 1999 está integrado en el marco institucional y jurídico de la Unión Europea en virtud de un protocolo anexo a los Tratados.

Los acuerdos de *Schengen* se han ido ampliando a lo largo del tiempo: Italia los firmó en 1990, España[381] y Portugal, en 1991, Grecia, en 1992, Austria lo hizo en 1995, Finlandia y Suecia en 1996, Dinamarca también en 1996 aunque con disposiciones especiales, y la República Checa, Estonia, Letonia, Lituania, Hungría, Malta, Polonia, Eslovenia y Eslovaquia en 2007. Irlanda y el Reino Unido participan sólo en parte en el acervo de *Schengen* ya que, por ejemplo, mantienen los controles en sus fronteras. Bulgaria, Chipre y Rumanía también aplican únicamente partes del acervo de *Schengen*, ya que para que se puedan eliminar los controles en las fronteras de esos países sigue siendo necesaria una Decisión del Consejo de la Unión Europea.

Cuatro países terceros forman asimismo parte del espacio *Schengen*, aunque su participación en la toma de decisiones es limitada: Islandia y Noruega desde 1996 y Suiza y Liechtenstein desde 2008.

Los Estados candidatos a la adhesión a la Unión Europea deben aceptar íntegramente el acervo de *Schengen* antes de su adhesión.

[380] DO L 239, de 22.09.2000

[381] Acuerdo de Adhesión de España, de 25.06.1991, al Convenio de Aplicación del Acuerdo de *Schengen* de 19 de junio de 1990. Instrumento de ratificación de 23.07.1993 *(BOE núm. 81, de 5 de abril de 1994. Corrección de erratas en BOE núm. 85, de 9 de abril)*. Disponible en: http://www.interior.gob.es/web/servicios-al-ciudadano/normativa/acuerdos-y-convenios/acuerdo-de-adhesion-de-espana-de-25-de-junio-de-1.

El espacio *Schengen* ha supuesto la creación de un Sistema de Información *Schengen* (SIS)[382], que es una base de datos compartida por todos los Estados miembros del espacio *Schengen*, a la cual se dedica el Título IV del Convenio, y que está formada por dos grupos de información: a) personas en búsqueda y captura[383], desaparecidos[384], necesitados de protección, o personas con la entrada prohibida en el espacio *Schengen*; y b) vehículos y objetos sustraídos o desaparecidos.

Todos los mecanismos y política a seguir en materia de protección de los datos de carácter personal del Sistema de Información *Schengen* están regulados en el Capítulo Tercero del Título IV del Convenio.

Al igual que ocurriera con Europol, también aquí se van a designar dos Autoridades en materia de protección de datos: una Autoridad Nacional y una Autoridad Común.

La Autoridad Nacional se encarga de *"ejercer un control independiente sobre el fichero de la parte nacional del Sistema de Información de Schengen y de comprobar que el tratamiento y la utilización de los datos introducidos en el Sistema de Integración de Schengen no atentan contra los derechos de la persona de que se trate".*[385] Esa Autoridad tendrá acceso al fichero de la parte nacional del Sistema de Información de *Schengen*. En el caso de España, la Autoridad Nacional encargada de controlar el SIS es la Agencia Española de Protección de Datos.[386]

La Autoridad de Control Común se encarga del control[387] de la unidad de apoyo técnico del Sistema de Información de *Schengen*, y a tal fin tiene acceso a dicha

[382] Artículo 93 Convenio Schengen: *"El Sistema de Información de Schengen tiene como objeto, con arreglo a lo dispuesto en el presente Convenio, preservar el orden y la seguridad públicos, incluida la seguridad del Estado, y la aplicación de las disposiciones del presente Convenio sobre la circulación de personas por los territorios de las Partes contratantes, con la ayuda de la información transmitida por dicho sistema".*

[383] Artículo 95 Convenio *Schengen.*

[384] Artículo 97 Convenio *Schengen.*

[385] Artículo 114 del Convenio *Schengen.*

[386] Artículo 10 del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos. BOE 106, de 4 de mayo de 1993.

[387] Artículo 115 del Convenio *Schengen:* "El control se ejercerá de conformidad con lo dispuesto en el presente Convenio, en el 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, teniendo en cuenta 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

unidad. Está formada por dos representantes de cada Autoridad Nacional de Control. También tendrá competencia "*para analizar las dificultades de aplicación o de interpretación que pudieran surgir con motivo de la explotación del Sistema de Información de Schengen, para estudiar los problemas que pudieran plantearse en el ejercicio del control independiente efectuado por las autoridades de control nacionales de las Partes contratantes o en el ejercicio del derecho de acceso al sistema, así como para elaborar propuestas armonizadas con vistas a hallar soluciones comunes a los problemas existentes*".

2.4.2.4 La Autoridad Común de Control Eurojust.

La Decisión del Consejo de la Unión Europea de 28 de febrero de 2002[388] creó Eurojust, un órgano con personalidad jurídica propia que pretende reforzar la lucha contra las formas organizadas de delincuencia fomentando y mejorando la coordinación y cooperación, las investigaciones y las actuaciones judiciales entre las autoridades competentes de los Estados miembros, en particular facilitando la ejecución de la asistencia judicial internacional y de las solicitudes de extradición; y apoyando en general a las autoridades competentes de los Estados miembros para dar mayor eficacia a sus investigaciones y actuaciones. Su ámbito de aplicación es el mismo en el que se mueve la Agencia Europol. La Decisión 2002/187/JAI del Consejo fue modificada por la Decisión 2009/426/JAI, de 16 de diciembre de 2008[389].

Eurojust está "*compuesto por un miembro nacional destacado por cada Estado miembro, conforme a su sistema jurídico, con la condición de fiscal, juez o funcionario de policía con competencias equivalentes"*.[390]

sector de la policía y con arreglo al Derecho nacional de la Parte contratante responsable de la unidad de apoyo técnico".

[388] Decisión 2002/187/JAI. DOCE de 6 de marzo de 2002, L63.

[389] DOUE de 4 de junio de 2009. L138.

[390] Artículo 2 Decisión 2002/187/JAI.

Se aprecia la madurez de la Decisión en materia de protección de datos de carácter personal (artículos 14 a 27), y ello porque su desarrollo es exhaustivo y perfectamente alineado con los principios, obligaciones y derechos previamente recogidos en la Directiva 95/46/CE y en el Reglamento (CE) 45/2001.

El artículo 23 de la Decisión[391] crea una Autoridad Común de Control independiente que controlará de manera colegiada las actividades de Eurojust a fin de garantizar que el tratamiento de los datos personales sea conforme a la Decisión, la cual está habilitada para acceder sin reservas a todos los ficheros en los que se tratan tales datos personales. Eurojust proporcionará a la Autoridad Común de Control cuanta información contengan los ficheros que solicite y le ayudará con cualquier otro medio a cumplir sus funciones.

La Autoridad Común de Control se reúne como mínimo una vez al semestre, y siempre en los tres meses siguientes a la presentación de un recurso, pudiendo ser convocada por su presidente cuando al menos dos Estados miembros así lo soliciten. Cada Estado miembro designa, con arreglo a su sistema jurídico, un juez que no sea miembro de Eurojust, o en caso de que así lo requiera su régimen constitucional o nacional, una persona que ejerza una función que le confiera la independencia adecuada para figurar en la lista de jueces que podrán actuar en la Autoridad Común de Control en calidad de miembro o de juez *ad hoc*. Una vez más, se recoge referencia expresa a la cualidad de la independencia con la que debe actuar la Autoridad de Control.

La Autoridad Común de Control estará compuesta por tres miembros permanentes Adicionalmente existirán también uno o varios jueces *ad hoc* para el estudio de recursos relacionado con datos personales procedentes del Estado miembro que les haya nombrado. Si la Autoridad Común de Control estima que una decisión adoptada

[391] Artículo 23.1 Decisión 2002/187/JAI: *"Se crea una Autoridad Común de Control independiente que controlará de manera colegiada las actividades de Eurojust mencionadas en los artículos 14 a 22, a fin de garantizar que el tratamiento de los datos personales sea conforme a la presente Decisión. En el cumplimiento de su cometido, la Autoridad Común de Control estará habilitada para acceder sin reservas a todos los ficheros en los que se tratan tales datos personales. Eurojust proporcionará a la Autoridad Común de Control cuanta información contengan los ficheros que solicite y le ayudará con cualquier otro medio a cumplir sus funciones".*

o un tratamiento de datos realizado por Eurojust no cumple las normas establecidas en la Decisión, se remitirá el dictamen a Eurojust, quien deberá dar cumplimiento a la decisión de la Autoridad Común de Control, pues sus decisiones son definitivas y vinculantes para Eurojust. Sus miembros están sujetos a la obligación de confidencialidad. La Autoridad común de Control informará una vez al año al Consejo.

El cumplimiento de las normas es la piedra angular de las actividades de la ACC. Por tanto, la ACC lleva a cabo inspecciones periódicas sobre el terreno y supervisa de manera permanente el seguimiento de todas las recomendaciones incluidas en los informes de inspección[392].

En la actualidad se está discutiendo el nuevo marco legal de la unidad Eurojust, en este caso un Reglamento.

2.4.2.5 La Autoridad Común de Control en el Sistema de Información Aduanero.

El Sistema de Información Aduanero (SIA) se creó mediante el Convenio establecido sobre la base del artículo K.3 del Tratado de la Unión Europea, relativo a la utilización de la tecnología de la información a efectos aduaneros, el 26 de julio de 1995[393], cuyo objetivo es *"contribuir a prevenir, investigar y perseguir las infracciones graves de las leyes nacionales, aumentando, mediante la rápida difusión de información, la eficacia de los procedimientos de cooperación y control de las administraciones aduaneras de los Estados miembros".*[394]

[392] Para más información: http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/jsb/jsb/The%20Role%20of%20the%20Joint%20Supervisory%20Body%20of%20Eurojust%20(leaflet)/Role-of-JSB-ES.pdf.

[393] Convenio establecido sobre la base del artículo K.3 del Tratado de la UE, relativo a la utilización de la tecnología de la información a efectos aduaneros. Bruselas, 26 de julio de 1995. DO C 316 de 27.11.1995. Disponible en: http://www.boe.es/diario_boe/txt.php?id=BOE-A-2000-20182.

[394] Idem. Artículo 2 del Convenio.

El Sistema de Información Aduanero es un banco central de datos accesible a través de terminales situadas en cada uno de los Estados miembros, y comprende exclusivamente aquellos datos, incluidos los datos personales, que sean necesarios para alcanzar el objetivo.

El acceso directo a los datos del SIA está limitado a las autoridades nacionales designadas por los Estados miembros y por la Comisión, de acuerdo con un listado que se remite a la Comisión, en la que también se indican las condiciones concretas que afectan al acceso por parte de cada autoridad a los datos[395].

Los Estados miembros únicamente podrán hacer uso de los datos obtenidos del sistema de información aduanero para alcanzar el objetivo enunciado en el Convenio. En todo caso, podrán utilizarse también para fines administrativos o de otra índole previa autorización y bajo las condiciones impuestas por el Estado miembro que los haya introducido en el sistema. Cualquier uso de dichos datos deberá ajustarse a las disposiciones legales y reglamentarias y los procedimientos del Estado miembro interesado y deberá tener en cuenta el principio 5.5 de Recomendación (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.

Excepcionalmente, algunas organizaciones internacionales o regionales pueden acceder al SIA. De la misma forma, se pueden transmitir, con carácter excepcional, información a otras autoridades nacionales o a terceros países.

Siguiendo el esquema de organismos anteriormente descritos, el Convenio SIA crea el doble sistema de Autoridades de Control: Una o varias Autoridades de Supervisión nacionales designadas por cada Estado miembro y una Autoridad de Supervisión Común.

Las Autoridades nacionales[396] responsables de la protección de los datos personales realizan una supervisión independiente de los datos personales incluidos en el

[395] Idem. Artículo 7 del Convenio.
[396] Idem. Artículo 17 del Convenio.

Sistema de Información Aduanero. Su labor se realizará siempre desde la independencia, y efectuará comprobaciones para asegurarse de que el tratamiento y la utilización de los datos del Sistema de Información Aduanero no conculcan los derechos de la persona interesada.

Por su parte, la Autoridad de Supervisión Común está facultada para supervisar el funcionamiento del Sistema de Información Aduanero, examinar todas las dificultades de aplicación o interpretación que puedan surgir en su funcionamiento, estudiar los problemas que puedan plantearse en el ejercicio de la supervisión independiente por parte de las autoridades nacionales de supervisión de los Estados miembros o en el ejercicio del derecho de acceso de las personas al Sistema y elaborar propuestas de solución común a los problemas[397].

La Autoridad de Supervisión Común desempeñará sus funciones de acuerdo con las disposiciones del propio Convenio, así como del Convenio de Estrasburgo de 1981 y tomando en consideración la Recomendación R (87) 15, de 17 de septiembre de 1987, del Comité de ministros del Consejo de Europa.

Para el cumplimiento de sus responsabilidades, la Autoridad de Supervisión Común tendrá acceso al Sistema de Información Aduanero, y sus informes serán remitidos a las autoridades.

2.4.3 Consejo Europeo de Protección de Datos. Hacia una Autoridad supraestatal.

El Consejo Europeo de Protección de Datos (CEPD) es un órgano de reciente creación que se establece en el nuevo Reglamento General de Protección de Datos (RGPD) y que actuará con total independencia, sin solicitar ni admitir instrucciones de nadie. Sustituye al Grupo de Trabajo del artículo 29 y lo dota de mayores competencias.

[397] Idem. Artículo 18 del Convenio.

Es un organismo consultivo, a la vez que mediador, con cualidades de Autoridad de control en cuanto que (previsiblemente) tomará decisiones vinculantes que permitan la coherencia del sistema.

Teniendo en cuenta que a fecha de estudio de este trabajo se barajan tres versiones del texto del RGPD, también son distintas las competencias y descripción del órgano según la versión.

En cuanto a la composición del órgano[398], estará formado por el director de una Autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de Datos. Para el caso de existir varias Autoridades de control en un mismo Estado miembro, éstas tendrán que elegir a una que será el representante común. La Comisión tendrá derecho a participar en las actividades y reuniones. Elegirá de entre sus miembros a un presidente y dos vicepresidentes[399], de los cuales uno será siempre el SEPD, salvo que sea presidente, siendo la duración de sus mandatos de cinco años.

Actualmente existe un gran debate en torno a si el CEPD debe tener o no personalidad jurídica. En la propuesta inicial de la Comisión esta cualidad no se preveía, ni tampoco el Parlamento lo hizo. Sin embargo, el Consejo sí ha recogido expresamente que "*gozará de personalidad jurídica*". Y en cuanto a la pertenencia del SEPD como miembro del CEPD, el Consejo considera que no debe tener derecho a voto.

La tarea fundamental del CEPD es velar por la aplicación coherente del Reglamento, para lo que cumplirá las siguientes funciones[400]:

- Asesorar a la Comisión sobre cualquier cuestión relativa a la protección de datos personales en la Unión, en particular sobre cualquier propuesta de modificación del RGPD.

[398] Artículo 64 Reglamento General de Protección de Datos, propuesta de la Comisión. http://register.consilium.europa.eu/doc/srv?f=ST+5853+2012+INIT&l=es.
[399] Artículo 69 RGPD, propuesta de la Comisión.
[400] Artículo 66 RGPD. Se analizarán los textos de la Comisión, Parlamento y Consejo.

Por su parte, el Parlamento propone una enmienda en la medida que entiende que el asesoramiento ha de ser no sólo a la Comisión, sino a las instituciones europeas.

Es esta una función, la de asesorar a los organismos comunitarios, que hasta ahora venía ejerciendo el Supervisor Europeo de Protección de Datos[401], por lo que en tanto no exista un cambio legislativo que lo modifique, dicha competencia será realizada por ambas instituciones: CEPD y SEPD.

- Examinar, a instancia propia o de la Comisión, o de uno de sus miembros, cualquier cuestión relativa a la aplicación del RGPD, emitiendo directrices, recomendaciones y mejores prácticas dirigidas a las autoridades de control, a fin de promover la aplicación coherente del Reglamento General de Protección de Datos.

La Comisión informará al CEPD sobre las medidas que haya adoptado a raíz de dichos instrumentos.

El texto propuesto por el Consejo otorga mayores competencias al CEPD ya que propone que formule directrices para las Autoridades de control relativas a la aplicación de los poderes de investigación y correctivos, así como de autorización y consultivos descritos en su propuesta de Reglamento y que son en esencia, mucho más amplios y detallados que los propuestos por la Comisión.

- Examinar la aplicación práctica de los mecanismos anteriores (directrices, recomendaciones y mejores prácticas) e informar periódicamente acerca de ello a la Comisión.

El Consejo además propone:

[401] Artículo 46.d) Reglamento (CE) 45/2001: *"asesorar a todas las instituciones y organismos comunitarios, tanto a iniciativa propia como en respuesta a una consulta, sobre todos los asuntos relacionados con el tratamiento de datos personales, especialmente antes de la elaboración por dichas instituciones y organismos de normas internas sobre la protección de los derechos y libertades fundamentales en relación con el tratamiento de datos personales".*

- que el CEPD aliente la elaboración de códigos de conducta y el establecimiento de mecanismos de certificación y de sellos y marcados de protección de datos que se recogen en los artículos 38 y 39 del RGPD[402];

- que acredite a los organismos de certificación así como para su revisión periódica;

- llevando también un registro público de los organismos acreditados y de los responsables o encargados del tratamiento acreditados establecidos en terceros países[403];

- en cuanto a los organismos y procedimientos de certificación, deberá especificar los requisitos del artículo 39 bis, apartado 3[404], con miras a la acreditación de los organismos de certificación en virtud del artículo 39;

- deberá emitir un dictamen destinado a la Comisión sobre el nivel de protección de los datos personales en terceros países u organizaciones internacionales, en especial los del artículo 41, que se refiere a las transferencias con una decisión de adecuación.

[402] El tema de los sellos y marcados de protección no es en sí una novedad, pues muchos sectores lo utilizan, si bien en protección de datos no se ha hecho nunca. El mayor valor que puede suponer su adopción por las empresas es su valor competitivo en un mercado único digital, en tanto que las diferencia produciendo una mayor confianza en el consumido. Pero existe un valor adicional, y es el menor impacto a nivel sancionador que pudiera tener una empresa ante una infracción. Estas circunstancias están por determinar.

[403] Artículo 66.1.c ter) RGPD versión Consejo, de 11.06.2015: *"realizará la acreditación de los organismos de certificación y su revisión periódica en virtud de lo dispuesto en el artículo 39 bis, y llevará un registro público de los organismos acreditados en virtud del artículo 39 bis, apartado 6, y de los responsables o los encargados del tratamiento acreditados establecidos en terceros países, en virtud del artículo 39, apartado 4".*

[404] Artículo 39 *bis*, apartado 3 RGPD versión Consejo, de 11.06.2015: *"La acreditación de los organismos de certificación a que se refiere el apartado 1 se llevará a cabo sobre la base de los criterios aprobados por la autoridad de supervisión competente de acuerdo con el artículo 51 o 51 bis o, de conformidad con el artículo 57, por el Consejo Europeo de Protección de Datos. En caso de acreditación de conformidad con la letra b del apartado 1, estos requisitos complementarán a aquellos previstos en el Reglamento 765/2008 y las normas técnicas que describen los métodos y procedimientos de los organismos de certificación".*

- Emitir dictámenes sobre los proyectos de decisión de las Autoridades de control en el mecanismo de coherencia del artículo 57 RGPD.

En cuanto al mecanismo de coherencia, tanto el Parlamento como el Consejo han presentado serias enmiendas al respecto.

El Parlamento entiende que en el marco de la cooperación y asistencia mutua entre Autoridades de control, el CEPD debe también emitir dictamen sobre qué autoridad debe ser la autoridad principal que se ocupa de un responsable o encargado del tratamiento en los siguientes casos: cuando los elementos presentados no permitan aclarar dónde se encuentra el establecimiento principal del responsable o del encargado del tratamiento; cuando las autoridades competentes no se pongan de acuerdo sobre cuál debe actuar como la principal; y cuando el responsable del tratamiento no esté establecido en la Unión y existan residentes de diferentes Estados miembros que se vean afectados por tratamientos en el ámbito de aplicación del Reglamento.

Por su parte, el Consejo considera que el CEPD adoptará una decisión vinculante en los siguientes casos:

- Cuando en los casos de cooperación entre la Autoridad de control principal y las demás afectadas, cualquiera de estas últimas formulen una objeción pertinente y motivada acerca del proyecto de decisión de la autoridad principal, o esta haya rechazado una objeción por no ser pertinente o no estar motivada.

- Cuando haya puntos de vista enfrentados sobre cuál de las Autoridades de control afectadas es competente para el establecimiento principal.

- Cuando una Autoridad de control competente no solicite dictamen al CEPD en los casos establecidos en el artículo 57.2 o no siga el dictamen del CEPD del artículo 58.

- Promover la cooperación y los intercambios bilaterales y multilaterales efectivos de información y de prácticas entre las Autoridades de control.

El Parlamento propone que se promueva la coordinación de operaciones conjuntas y otras actividades comunes, cuando así lo decida a solicitud de una o varias Autoridades de control.

- Promover programas de formación comunes y facilitar intercambios de personal entre las Autoridades de control, así como entre éstas y Autoridades de control de terceros países u organizaciones internacionales.

- Promover el intercambio de conocimientos y documentación sobre la legislación y prácticas en materia de protección de datos con las Autoridades de control a escala mundial.

El Parlamento ha realizado notables aportaciones, entendiendo que el CEPD debe además ofrecer:

  - un dictamen a la Comisión respecto de los actos delegados y de ejecución basados en el RGPD;

  - un dictamen sobre los códigos de conducta elaborados a escala de la Unión según lo establecido en el artículo 38.4[405];

  - un dictamen sobre los criterios y requisitos aplicables a los mecanismos de certificación en materia de protección de datos a los que se refiere el artículo 39.3[406];

[405] Artículo 38.4 RGPD, propuesta de la Comisión: *"La Comisión podrá adoptar actos de ejecución para decidir que los códigos de conducta y las modificaciones o ampliaciones de códigos de conducta existentes que les sean sometidos con arreglo a lo dispuesto en el apartado 3 tienen validez general dentro de la Unión. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 87, apartado 2".*

[406] Artículo 39.3 RGPD, propuesta de la Comisión: *"La Comisión podrá establecer normas técnicas para los mecanismos de certificación y los sellos y marcados de protección de datos, y mecanismos para promover y reconocer los mecanismos de certificación y los sellos y marcados de protección*

- el mantenimiento de un registro público electrónico de los certificados válidos e inválidos de conformidad con el artículo 39.1 nonies[407];

- proporcionar asistencia a las autoridades de control nacionales, a petición de ellas;

- establecer y publicar una lista de los tipos de operaciones de tratamiento que deben ser objeto de consulta previa según el artículo 34[408];

- mantener un registro de las sanciones impuestas a los responsables o encargados del tratamiento por parte de las autoridades de control competentes.

Por su parte, el Consejo considera que entre las funciones del CEPD, además de las descritas en el texto de la Comisión, estaría llevar un registro electrónico de acceso público de las decisiones adoptadas por las Autoridades de control y los órganos jurisdiccionales sobre los asuntos tratados en el mecanismo de coherencia.

El Consejo Europeo de Protección de Datos elaborará además anualmente un informe sobre la situación en materia de protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales en la Unión y en terceros

de datos. Dichos actos de Ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 87, apartado 2".

[407] Artículo 39.1. nonies, enmiendas presentadas por el Parlamento, de 12.03.2014: *"El Consejo Europeo de Protección de Datos establecerá un registro público electrónico en el que el público podrá ver todos los certificados válidos e inválidos expedidos en el Estado miembro".*

[408] Artículo 34.2 RGPD describe las operaciones que deben ser objeto de consulta previa: *"El responsable o el encargado del tratamiento que actúe por cuenta de aquel deberán consultar a la autoridad de control antes de proceder al tratamiento de datos personales a fin de garantizar la conformidad del tratamiento previsto con el presente Reglamento y, sobre todo, de atenuar los riesgos para los interesados cuando: a) una evaluación del impacto en la protección de los datos, tal como dispone el artículo 33, indique que es probable que las operaciones de tratamiento, por su naturaleza, alcance o fines, entrañen un elevado nivel de riesgos específicos; o b) la autoridad de control considere necesario proceder a una consulta previa en relación con las operaciones de tratamiento que probablemente entrañen riesgos específicos para los derechos y libertades de los interesados en razón de su naturaleza, alcance y/o fines, y hayan sido especificadas con arreglo al apartado 4".*

países.[409] Este informe incluirá el examen de la aplicación práctica de las directrices, recomendaciones y mejores prácticas antes descritas.

También adoptará su reglamento interno y sus disposiciones de funcionamiento[410], y determinará la distribución de tareas entre presidente y vicepresidentes.

Serán tareas del Presidente convocar las reuniones del Consejo Europeo de Protección de Datos y preparar su agenda, así como garantizar el cumplimiento puntual de las tareas, en especial en lo relativo al mecanismo de coherencia.

En cuanto a la Secretaría, será el Supervisor Europeo de Protección de Datos el encargado de la misma, en los términos ya descritos en el apartado dedicado a este organismo[411].

Del análisis de las funciones y la composición del Consejo Europeo de Protección de Datos deducimos que es un órgano que podríamos denominar de coordinación entre las Autoridades de control nacionales y entre las autoridades y la Comisión. Son muchas las funciones que presenta de asesoramiento, control e investigación, por lo que pareciera encontrase a camino entre un órgano consultivo y una autoridad de control.

Los textos del Reglamento General de Protección de Datos, en los artículos correspondientes a los mecanismos de cooperación y coherencia resultan en ocasiones farragosos y difíciles de entender, y es de resaltar la solicitud formulada por el Grupo de Trabajo del artículo 29 de hacer un texto claro, sencillo y fácil de entender[412].

También el texto presenta multitud de competencias para la Comisión que ejercería a través de sus actos delegados (la aplicación del nuevo mecanismo de coherencia, la evaluación de la adecuación de terceros países, la preparación de medidas de

[409] Artículo 67 RGPD.
[410] Artículo 68 RGPD.
[411] Apartado 2.4.2.1.- Funciones y competencias del SEPD.
[412] Carta del GT 29 a la Comisaria *Vera Jourovà* de 17.06.2015. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_letter_from_the_art29_wp_on_trilogue_to_msjourova_en.pdf.

ejecución), que entendemos debieran ser acometidas por el propio Consejo Europeo de Protección de Datos y no por la Comisión, para lo que indudablemente el CEPD deberá tener personalidad jurídica. El nuevo modelo normativo en protección de datos debe ser más próximo a los ciudadanos, con mayor relación con su Autoridad de control, en la que ésta no sea un organismo que imponga miedo a los ciudadanos, sino al contrario, debe ser una administración colaborativa que les ayude a entender y a relacionarse bajo el cumplimiento siempre del derecho a la protección de datos.

Pero de nada servirá un nuevo modelo de gobierno en el que se predica la armonización normativa si no existe un organismo que realmente coordine a las Autoridades de control y tenga competencias reales sobre ellas, con poderes consultivos, de investigación y de intervención necesarios para llevar a cabo políticas y cumplimiento de la norma de forma homogénea en todo el territorio de la Unión Europea, y donde las Autoridades de control estén también supervisadas. Sus decisiones deberán ser vinculantes y siempre recurribles ante la autoridad judicial competente. No es posible instaurar un mecanismo de coherencia sin tener en última instancia un organismo capaz de tomar cuantas decisiones sean necesarias para que por las Autoridades de control nacionales (que están acostumbradas a ser soberanas) se ejecuten las decisiones tomadas por un organismo jerárquicamente superior. La pérdida de parte de la soberanía es consustancial a la creación de una organización supranacional como es la Unión Europea. Entendiendo que el proceso es paulatino y lento, consideramos que ha llegado la hora de armonizar *de facto* la normativa y aplicación del derecho a la protección de datos, con las cesiones que ello suponga, para lo que debe existir un organismo jerárquicamente superior que pueda desarrollar, coordinar y ejecutar una política común entre las Autoridades de control. Y ese organismo puede ser el Consejo Europeo de Protección de Datos, pero no la Comisión Europea, que es el gobierno de la Unión Europea, órgano ejecutivo y garante del cumplimiento de los Tratados, y sus cometidos no son los descritos anteriormente, sino otros.

Existen a nivel europeo otros organismos similares al CEPD, como es el Consejo de Supervisión del Mecanismo Único de Supervisión[413] del Banco Central Europeo (BCE), formado por un presidente, dos vicepresidentes, cuatro representantes del BCE y representantes de los supervisores nacionales[414]. Tras la reciente crisis financiera en Europa se hizo necesario un organismo que supervisara a los bancos coordinadamente, a través de los propios supervisores de cada uno de ellos, es decir los bancos centrales, y ello porque la conexión entre los bancos es tan alta que ante cualquier situación problemática existe un alto riesgo de contagio de unos a otros. Los equipos conjuntos de supervisión están formados por personal del BCE y de las autoridades nacionales bancarias, los cuales realizan una evaluación continua del perfil de riesgo y de la adecuación de solvencia y de liquidez de las entidades, y serán los responsables de preparar las propuestas de decisión para ser elevadas al Consejo de Supervisión. Estos equipos dan soporte a las inspecciones in situ, recopilan y transmiten toda la información que requieran y colaboran en los procesos sancionadores.

2.4.4 La Independencia.

Del estudio de las Autoridades de control analizadas, podemos extraer las características que entendemos deben servir de parámetros para la creación de cualesquiera Autoridades de control de protección de datos[415]:

- Independencia.
- Poderes consultivos, de investigación y de intervención.

[413] El Mecanismo Único de Supervisión (MUS) se compone del Banco Central Europeo (BCE) y de las autoridades nacionales competentes (ANC) de los Estados miembros participantes, por lo que combina las fortalezas, la experiencia y los conocimientos especializados de estas instituciones. http://www.bde.es/bde/es/areas/supervision/sup/Mecanismo_Unico_/El_modelo_de_sup/El_modelo_de_supervision.html.

[414] Para mayor información, consultar https://www.bankingsupervision.europa.eu/organisation/whoiswho/supervisoryboard/html/index.en.html

[415] Sobre las Autoridades de control, SALVADOR MARTÍNEZ, M. *Autoridades independientes*, Ariel, Barcelona, 2002.

- Capacidad procesal para participar en procedimientos judiciales, de interponer acciones ante las autoridades judiciales ante violaciones en materia de protección de datos y de hacer frente a las quejas.
- Decisiones recurribles ante los tribunales de justicia.
- Experiencia y competencia notorias para el cumplimiento de la labor de los miembros.
- Disposición de los recursos humanos y financieros necesarios para el ejercicio de sus funciones, otorgados por su autoridad presupuestaria.
- Disposición de una Secretaría y miembros nombrados por el organismo.
- Secreto profesional durante y después del mandato.
- Sujeción del organismo a mecanismos de control financieros y judiciales.

De todas estas características, es la independencia el elemento clave en la configuración del derecho a la protección de datos. Tal y como analizaba *Peter Huskinx*[416], el principio de "'supervisión independiente" y la existencia de "autoridades de supervisión independientes" se han convertido, al menos a nivel europeo, en un elemento constitucional del derecho a la protección de datos en una sociedad democrática, y a la vez una característica asociada al cumplimiento y a la "protección eficaz". Pero también considera *Huskinx*, y es un elemento realmente interesante, que es crucial para las autoridades de supervisión independientes cuestionarse regularmente su propia eficacia y mejorar su rendimiento.

La cualidad y descripción de la independencia en la Autoridad de control de protección de datos viene siendo una constante desde la Directiva 95/46/CE. Así, vemos que aparece en los siguientes textos normativos:

- Artículo 16 del Tratado de la Unión Europea[417];

[416]HUSKINX, P. "The Role of Data Protection Authorities", en PÉREZ ASINARI, M.V. & PALAZZI, P. (Eds) *Défis su droit à la protection de la vie privée. Challenges of privacy and data protection law*, Bruselas, Bruylant, 2008, p 561-568.

[417] Artículo 16 TUE: *"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*

- Artículo 28 de la Directiva 95/46/CE[418];
- Protocolo Adicional del Convenio 108 del Consejo de Europa[419];
- Artículo 8 de la Carta de Derechos Fundamentales[420];
- Considerandos 2, 3, 5, 21, 23, 24, 25 y 26 (hasta diez veces dice textualmente *"autoridad de control independiente*") del Reglamento 45/2001;
- Artículo 1.2 del Reglamento 45/2001[421];
- Capítulo V del Reglamento 45/2001[422];
- Artículo 41.1 del Reglamento 45/2001[423];
- Artículos 42[424] y 44[425] del Reglamento 45/2001;
- Artículo 3[426]; y 15[427] del Reglamento Interno del Supervisor Europeo de Protección de Datos;

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".

[418] Artículo 28 Directiva 95/46/CE: *"1. Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva. Estas autoridades ejercerán las funciones que les son atribuidas con total independencia"*.

[419] Artículo 1.3: *"Las Autoridades de Control ejercerán sus funciones con completa independencia".* CETS nº 181, 2001.

[420] Artículo 8.3: *"El respeto de estas normas quedará sujeto al control de una autoridad independiente"*. DO C 303 de 14/12/2007.

[421] Artículo 1 Reglamento (CE) 45/2001: "2. La autoridad de control independiente establecida por el presente Reglamento, en lo sucesivo denominada «Supervisor Europeo de Protección de Datos», supervisará la aplicación de las disposiciones del presente Reglamento a todas las operaciones de tratamiento realizadas por las instituciones y organismos comunitarios".

[422] Capítulo V del Reglamento (CE) 45/2001: *"Autoridad de control independiente: El Supervisor Europeo de Protección de Datos"*

[423] Artículo 41 del Reglamento (CE) 45/2001*"1. Se instituye una autoridad de control independiente denominada «Supervisor Europeo de Protección de Datos»*.

[424] Artículo 42 del Reglamento (CE) 45/2001:*"El Supervisor Europeo de Protección de Datos será elegido entre personas cuya independencia esté fuera de toda duda y que posean una experiencia y competencia notorias para el cumplimiento de las funciones de Supervisor Europeo de Protección de Datos, como pertenecer o haber pertenecido a las autoridades de control mencionadas en el artículo 28 de la Directiva 95/46/CE".*

[425] Artículo 44 del Reglamento (CE) 45/2001: "*1. El Supervisor Europeo de Protección de Datos actuará con total independencia en el ejercicio de sus funciones. 2. En el ejercicio de sus funciones el Supervisor Europeo de Protección de Datos no solicitará ni admitirá instrucciones de nadie. 3. El Supervisor Europeo de Protección de Datos se abstendrá de cualquier acción incompatible con sus funciones y de desempeñar, durante su mandato, ninguna otra actividad profesional, sea o no retribuida. 4. Tras la finalización de su mandato el Supervisor Europeo de Protección de Datos actuará con integridad y discreción en lo que respecta a la aceptación de nombramientos y privilegios.".*

[426] DO L 273, artículo 3*: "Independencia, buen gobierno y buena conducta administrativa. 1. De conformidad con el artículo 44 del Reglamento, el supervisor actuará con plena independencia en el ejercicio de sus funciones. 2. El supervisor garantizará el buen funcionamiento de los servicios*

- Considerandos 92, 92bis, 95 y 121 del Reglamento General de Protección de Datos, así como artículo 4.19), 41.2b) y capítulo VI -artículos 46 a 50- (versión Comisión).

La situación de las Autoridades de control en los *Länder* alemanes abrió la puerta a un pronunciamiento por parte del Tribunal de Justicia de la Unión Europea en 2010[428] donde tuvo que interpretar y sentenciar sobre el concepto de independencia descrito en el artículo 28 de la Directiva 95/46/CE. Es el asunto C-518/07 entre la República Federal de Alemania y la Comisión Europea.

En Alemania las Autoridades de control son distintas según sean encargadas de vigilar datos del sector público o privado. El tratamiento de datos personales efectuado por los organismos públicos se vigila, a escala federal, por el delegado federal para la protección de datos[429] y, en los *Länder,* por los delegados para la protección de los *Länder*[430]. Pero la estructura de las autoridades encargadas de vigilar el tratamiento de los datos por el sector no público varía de un *Land* a otro, y están sometidas a la tutela del Estado, por lo que la Comisión Europea (apoyada en su opinión por el SEPD) entendía que ante esta circunstancia la República Federal de Alemania incumplía las obligaciones que le incumben en virtud del artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46/CE[431] y por lo tanto había adoptado incorrectamente su normativa nacional a la exigencia de «total independencia» de las autoridades encargadas de garantizar la protección de estos datos. Inicialmente la Comisión envió un escrito de requerimiento, contestando la República Federal de Alemania que su sistema de control era conforme a la Directiva. Posteriormente la Comisión envió un Dictamen motivado reiterando su

disponibles para el ejercicio de las funciones mencionadas en el artículo 1, teniendo en cuenta los principios de buen gobierno, buena conducta administrativa y buena gestión".

[427] *"Principios rectores y valores clave. 1. El SEPD actuará al servicio del interés público como organismo con autoridad, experto, independiente y fiable en el ámbito de la protección de datos, a nivel europeo. Las intervenciones del SEPD estarán basadas en los principios de imparcialidad, integridad, transparencia y pragmatismo".*

[428] STJUE de 09.03.2010. Asunto C-518/07. Disponible en: http://curia.europa.eu/juris/document/document.jsf?text=&docid=79752&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=285506.

[429] *Bundesbeauftragter für den Datenschutz und die Informationsfreiheit.*

[430] Landesdatenschutzbeauftragte.

[431] DO L 281, p. 31.

imputación y la contestación fue idéntica. En base a ello, la Comisión se vio obligada a interponer recurso ante el Tribunal de Justicia de la Unión Europea, interviniendo el Supervisor Europeo de Protección de Datos en apoyo de las pretensiones de la Comisión.

El debate se centró en el alcance de la expresión "total independencia" que predica el artículo 28 de la Directiva 95/46/CE. Para la Comisión y el SEPD debía interpretarse en el sentido de que dichas autoridades deberían estar exentas de toda influencia, tanto si era ejercida por otras autoridades como si era ajena a la Administración, entendiendo pues que la tutela del Estado a la que están sometidas las autoridades encargadas de controlar el respeto de la normativa en materia de protección de datos en el sector no público en Alemania suponía un incumplimiento de la norma. Por el contrario, la República Federal de Alemania hacía una interpretación más estricta de la expresión "total independencia", presuponiendo que es una independencia funcional, y que la tutela que ejerce el Estado no constituye influencia externa alguna.

Para el Tribunal el término «independencia» se refiere normalmente al estatuto que le garantiza la posibilidad de actuar con plena libertad, a resguardo de cualquier tipo de instrucciones o presiones, y al venir reforzado por el adjetivo «total», implica una facultad de decisión exenta de toda influencia externa a la Autoridad de control, ya sea directa o indirecta.

Entiende también el Tribunal que el objeto de la Directiva es garantizar la libre circulación de los datos entre los Estados miembros[432] necesaria para el funcionamiento del mercado interior. Pero que esa libre circulación de datos personales puede vulnerar el derecho al respeto de la vida privada reconocido en el artículo 8 del Convenio 108 del Consejo de Europa y en los principios generales del derecho comunitario, por lo que las Autoridades de control del artículo 28 son guardianas de los mencionados derechos y libertades fundamentales; y, como señala el considerando 62 de dicha Directiva, *"se estima que su creación en cada uno de los*

[432] Sentencia del TJUE de 20.05.2003, *Österreichischer Rundfunk y otros*, C‑465/00, C‑138/01 y C‑139/01, apartados 39 y 70.

Estados miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales", siendo que la garantía de independencia no se ha establecido para conceder un estatuto particular a esas autoridades mismas o a sus agentes, sino para reforzar la protección de las personas y de los organismos afectados por sus decisiones. De lo anterior resulta que, en el ejercicio de sus funciones, las Autoridades de control deben actuar con objetividad e imparcialidad, y, para ello, han de estar a resguardo de toda influencia externa, incluida la ejercida directa o indirectamente por el Estado o por los Länder, y no solamente de la de los organismos sujetos a control.

Analiza el Tribunal la comparativa entre los sistemas descritos tanto en la Directiva 95/46/CE como en el Reglamento (CE) núm. 45/2001, entendiendo que al igual que existen órganos de control a escala nacional, también existe a escala comunitaria un órgano de control encargado de vigilar la aplicación de la normativa en materia de protección de datos como es el SEPD, para lo que Tribunal examina el contenido del artículo 44 del Reglamento (CE) núm. 45/2001 en lo que se refiere a la descripción de la independencia del organismo, aplicando un paralelismo entre ambas autoridades de control, las nacionales y la comunitaria, las cuales se basan en el mismo concepto general y por lo tanto han de interpretarse de manera homogénea.

Subraya el Tribunal que *"la mera posibilidad de que las autoridades de tutela puedan ejercer influencia política sobre las decisiones de las autoridades de control es suficiente para obstaculizar el ejercicio independiente de las funciones de éstas*", debiendo estar *"por encima de toda sospecha de parcialidad".*

Finalmente, el TJUE sentenció que el sistema de Autoridades de control de los *Länder* no es independiente en el sentido del artículo 28 de la Directiva 95/46/CE[433].

[433] Sentencia del TJUE de 20.05.2003, *Österreichischer Rundfunk* y otros, C‑465/00, C‑138/01 y C‑139/01*: "En virtud de todo lo expuesto, el Tribunal de Justicia (Gran Sala) decide: Declarar que la República Federal de Alemania ha incumplido las obligaciones que le incumben en virtud del artículo 28, apartado 1, párrafo segundo, 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, al someter a la tutela del Estado a las autoridades de control encargadas de vigilar en los diferentes Länder el*

Más reciente es la sentencia del TJUE de 2014 que enfrentó a la Comisión con Hungría[434], en la que la Comisión Europea solicitaba al Tribunal declarase que Hungría había incumplido las obligaciones que le incumben en virtud de la Directiva 95/46/CE al poner fin antes de tiempo al mandato de la Autoridad de control de la protección de datos personales. La Autoridad de control del gobierno húngaro tenía un mandato por seis años, pero en ese ínterin la normativa fue modificada para, según el gobierno húngaro, adaptarse a la Directiva 95/46/CE, creando una nueva Autoridad de protección de datos, lo que hizo que el mandato de la anterior Autoridad de control expirara antes de lo previsto. Al igual que ocurriera en el caso de los *Länder* de la República Federal de Alemania, la Comisión remitió un escrito de requerimiento a Hungría, en el que exponía estimaba había infringido el artículo 28, apartados 1 y 2, de la Directiva 95/46 por varias razones: por finalizar el mandato del Supervisor antes de lo establecido, por no consultarle a éste acerca del proyecto de la nueva Ley de protección de datos y por contemplar en la nueva Ley demasiadas posibilidades de poner fin al mandato del presidente de la Autoridad, reconociéndole a este respecto atribuciones al Presidente de la República y al Primer Ministro. Hungría contestó negando la infracción, y la Comisión envió un Dictamen motivado en el que reiteraba su preocupación sobre la finalización anticipada del mandato y las atribuciones al Presidente y Primer Ministro. Consecuencia de ello la Comisión interpuso recurso ante el TJUE con la intervención del SEPD en apoyo de sus pretensiones.

El gobierno húngaro negó haber cometido infracción alguna por tres razones: porque el requisito de la independencia no se extiende a la decisión de un Estado miembro sobre el modelo institucional de la Autoridad de control, porque la Directiva otorga libertad para definir la estructura y duración del mandato, y porque la interpretación del artículo 28 de la Directiva, según la Comisión y el SEPD, supondría la prohibición de renovación de los cargos. Considera Hungría al respecto que *"si se*

tratamiento de datos personales efectuado por los organismos no públicos y las empresas públicas que compiten en el mercado (öffentlich‑rechtliche Wettbewerbsunternehmen), y al haber adaptado así incorrectamente su normativa nacional a la exigencia de que dichas autoridades ejerzan sus funciones con «total independencia».

[434] STJUE de 08.04.2014, Asunto C-288/12, Comisión vs Hungría. Disponible en: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150641&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=285061.

siguiera la tesis de la Comisión, debería interpretarse que la Directiva 95/46 excluye igualmente que el mandato de la persona que está al frente de la autoridad de control pueda renovarse o que esta persona pueda ejercer otro cargo público electivo. En efecto, tal tesis implicaría que la esperanza de que se renueve el mandato o de que se pueda desempeñar otro cargo podría suponer un estímulo para que el presidente de la autoridad de control satisfaga las expectativas reales o supuestas del poder político para favorecer su carrera posterior".

La clave en este procedimiento estaba en determinar si la obligación de que la actuación de la Autoridad de control sea independiente supone el deber del Estado miembro de respetar la duración del mandato de tal autoridad, sin que pueda estar justificada la finalización del mismo anticipadamente por el cambio del modelo institucional. Nuevamente, el Tribunal de Justicia descarta que la independencia funcional sea suficiente para cumplir con la independencia reclamada en el artículo 28 de la Directiva, ya que dicha independencia funcional no basta para proteger a una Autoridad de control de las influencias externas, entendiendo finalmente que la normativa húngara vulneró el artículo 28 de la Directiva 95/46/CE.

Compartiendo con el Tribunal la tesis que avala que la mera independencia funcional no supone una independencia total, es relevante el análisis (en el que ellos no se posicionan) del estado húngaro en cuanto que la independencia total podría suponer la imposibilidad de renovación del cargo de las Autoridades de control, entendemos que aunque el sistema sea absolutamente transparente, equitativo e imparcial, no es menos cierto que los seres humanos pueden modificar sus conductas por un sentimiento interior. Es decir, es factible la posibilidad de que una persona éticamente intachable ante los deseos lógicos de continuar en un puesto o de conseguir el beneplácito de quien tiene que nombrarlo pueda tener conductas alejadas de la imparcialidad (aún sin ser consciente de ello) que sean deseadas o esperadas por estos últimos. Por ello consideramos que la no renovación de los cargos de las Autoridades de control debería suponer una referencia a estandarizar en aras de conseguir la independencia total.

Traemos también aquí a colación el debate acerca del nombramiento de la Autoridad de Control. Explicábamos anteriormente el procedimiento para elegir al Supervisor y Supervisor adjunto, el cual es absolutamente transparente e imparcial: lista de candidatos, concurso de méritos y selección por dos organismos. Cabe pensar que los nombramientos producidos directamente por los gobiernos se alejan de la independencia que se predica, a pesar del control posterior y de la independencia real con la que se lleve a cabo el cargo. Un nombramiento realizado por el gobierno de un país puede (aunque no lo sea) esperar desde ambos lados (elector y elegido) un comportamiento afín a unos determinados intereses políticos.

En 2013, la Agencia de los Derechos Fundamentales Europea, FRA, publicó un "Informe sobre el acceso a las vías de recurso en materia de protección de datos en los Estados miembros de la Unión Europea"[435], donde en línea con su investigación analiza las Autoridades de control. Pues bien, sus conclusiones son claras: *"Es fundamental que las autoridades de protección de datos no dependan de ningún control externo, en relación tanto con la asignación y el gasto de fondos como con la contratación de personal. Tal independencia reviste especial importancia, ya que las autoridades de protección de datos también tienen que ocuparse de las infracciones cometidas por el Estado. Además, deben estar dotadas de procedimientos adecuados, atribuciones suficientes y recursos apropiados, incluidos profesionales cualificados, para hacer uso de estos procedimientos y atribuciones"*

Del análisis de las referencias normativas y doctrinales, de la jurisprudencia del Tribunal de Justicia de la Unión Europea y de nuestro estudio, deducimos que la independencia es un elemento clave en la configuración del derecho a la protección de datos, y que presupone las siguientes características:

- estar fuera de toda duda;
- no admitir ni solicitar instrucciones de nadie;
- no tener influencia exterior alguna, ni directa ni indirecta;

[435] El informe del FRA está disponible en: http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en.pdf.

- no ejercer ninguna función incompatible con sus funciones;
- no desempeñar durante el mandato ninguna otra actividad profesional, sea retribuida o no;
- nombramientos realizados por el Parlamento con mayoría cualificada;
- determinación legal de las cualificaciones, procedimiento de nombramiento, duración, carácter o no renovable del cargo o incompatibilidades durante y después del cargo.
- finalización del mandato al expirar el plazo o por dimisión o jubilación obligatoria;
- cargos no renovables;
- actuar con integridad y discreción en lo que respecta a nuevos nombramientos y privilegios a la finalización del mandato;
- deber de secreto profesional durante y después del mandato;
- dotación de recursos (financieros, técnicos, humanos, infraestructuras y locales…) necesarios para la realización eficaz de sus tareas;
- disposición de un presupuesto anual propio, público e independiente;
- personal propio sujeto a la propia Autoridad de control;
- personal con titulación, experiencia y aptitudes necesarias para el cumplimiento de sus funciones y el ejercicio de sus poderes.

3 CAPÍTULO II. Comparativa con la Privacidad y Supervisión en EEUU.

Los modelos europeo y americano en materia de protección de datos distan mucho de ser similares, pero inexorablemente están llamados a entenderse. No existe globalización ni desarrollo que valga si EEUU y Europa no se entienden. Así pues, es de obligado cumplimiento para ambas partes multiplicar los esfuerzos hasta alcanzar acuerdos, y no es posible lograrlo si no son capaces de empatizar. EEUU y Europa, Europa y EEUU deberán buscar sus similitudes y allanar sus diferencias, especialmente buscando y hallando lo bueno que existe a ambos lados del Atlántico.

Dada la situación actual donde los pilares de la transferencia de datos entre ambos territorios han sido desautorizados por el Tribunal de Justicia de la Unión Europea, urge más que nunca dicho entendimiento.

3.1 La *Privacy*.

El concepto de la *privacy* nació en los Estados Unidos. Hasta finales del siglo XIX no se le prestó atención al concepto de vida privada, donde las amenazas a ésta eran entendidas como amenazas a la propiedad, la cual era el origen de todos los derechos.[436]. La vida íntima o privada aparecía como una parcela más dentro de la propiedad[437].

[436] LOCKE, JOHN escribió en su Segundo Tratado sobre el Gobierno Civil, (traducción C. Mellizo, Alianza Editorial, Madrid, 1994., núm. 44, p. 70): *"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".*

[437] El derecho anglosajón incorpora a su jurisprudencia la máxima "*a man´s house is his castle*" (la casa/el hogar del hombre es su castillo). Vease. HAFETZ, JONATHAN L, *"A Man's Home is His Castle?": Reflections on the Home, the Family, and Privacy During the Late Nineteenth and Early Twentieth Centuries*, 8 Wm. & Mary J. Women & L. 175, 2002, p. 175-242. También se puede consultar en: http://scholarship.law.wm.edu/wmjowl/vol8/iss2/2.

Fueron dos abogados americanos quienes concibieron por vez primera el derecho a la privacidad hasta llevarlo a su reconocimiento constitucional. *Warren* y *Brandeis*[438] definieron la esfera privada como fundamento de la libertad individual en la era moderna, para lo cual entendían que la ley debía evolucionar en respuesta a los cambios tecnológicos. El detonante fue la intromisión en la privacidad que suponía el hacer "fotografías instantáneas", tal y como ellos las denominaban, sin que las personas fueran conocedoras ni prestaran su consentimiento para su realización, infiriéndolo pues como una intromisión en su privacidad. *Warren* y *Brandeis* compararon la privacidad a la ley de difamación, a los derechos de propiedad física, la propiedad intelectual y la ley de contrato. Fue este un concepto nuevo y ampliamente debatido doctrinal y jurisprudencialmente, y en consecuencia no pacífico.

El eminente jurista *William Prosser*[439], en su obra "*Privacy*"[440], entendió que la privacidad estaba constituida por cuatro agravios (*tort*) distintos: Intrusión en la intimidad o la soledad, o en los asuntos privados; la divulgación pública de hechos privados embarazosos; la imagen falsa de la persona ante el público; y la apropiación del nombre o imagen[441]. Esta posición ha sido muy influyente y permanece aún

Por su parte, EEUU también incorpora este principio a su jurisprudencia a través de la sentencia del juez Bradley declarando "*the sanctity of a man's home and the privacies life*", conectando por primera vez las garantías de la Cuarta y Quinta enmiendas frente a la invasión gubernamental de la privacidad individual para obtener información reservada de la persona a través del registro ilegal de su domicilio al objeto de utilizarla como evidencia contra ella: "La esencia misma de la libertad y seguridad constitucional se ve afectada ante cualquier invasión por parte del gobierno y de sus agentes de la santidad del hogar de la persona y de la privacidad de su vida. No es la rotura de sus puertas, o el registro de sus cajones lo que constituye la esencia del delito, sino la invasión de su inderogable derecho a la libertad y seguridad personal y a la propiedad privada". Boyd v. United States, 116 U.S. 616, 630 (1886).
Se puede consultar en: http://caselaw.findlaw.com/us-supreme-court/116/616.html.

[438] WARREN, S.D. y BRANDEIS, L. *The Right to Privacy.* Harvard Law Review, volumen IV, núm. 5, 1890, P.194-220.
Disponible en:
http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

[439] Para mayor análisis de las teorías de *Prosser,* ver SOUVIRÓN MORENILLA, J.M. "Privacidad y derechos fundamentales", en VVAA, Introducción a los derechos fundamentales, vol. III. Ministerio de Justicia, Madrid, 1998, p. 1873-1890.

[440] PROSSER, W. *Privacy*, 48 Cal. L. Rev. 383. 1.960.
Disponible en: http://scholarship.law.berkeley.edu/californialawreview/vol48/iss3/1.

[441] Los defensores del modelo actual americano presuponen que muchos defensores de la privacidad olvidan esta protección que debe ser dada a través de los tribunales, pues para ellos el litigio es sin duda mejor escenario que la regulación administrativa como medio para proteger la privacidad.

como herramienta útil para clasificar los distintos objetos del ámbito de la privacidad en el campo de los daños civiles. Pero su posición también ha sido muy criticada, entre otros por *Edward Bloustein*[442] que se distanciaría bastante de esta teoría, asumiendo una posición normativa e intentando buscar cuál es el interés general que ampara el derecho al reconocer la vida privada como objeto de protección[443].

Una de las grandes aportaciones doctrinales en esta materia vino de la mano de Alan F. *Westin*[444] con el concepto de "autodeterminación" (*self determination*), concepto que posteriormente ha sido acuñado en varios ordenamientos jurídicos como el alemán o el español[445]. Tal y como reconoce Piñar Mañas[446], *Westin* identificó cuatro tipos de privacidad, que *Pedersen* amplió hasta cinco: soledad, aislamiento, reserva, intimidad y anonimato.

Todos estos autores son estadounidenses, y su debate acerca de la *privacy* ha sido constante. Avanzando en el tiempo, y ya con internet sobre nuestros escritorios, *Paul M. Schwartz*[447], para quien la promulgación de una ley federal sería un paso decisivo en la construcción de la democracia, reconocía que las normas necesarias deben establecer cuatro requisitos: 1.- obligaciones claramente definidas que limitan el uso de los datos personales; 2.- sistemas de procesamiento de datos transparentes; 3.- atribución de derechos a los individuos y 4.- la supervisión externa. Considera *Schwartz* que ni la autorregulación del mercado, ni la industria, pueden desarrollar estas cuatro prácticas.

---

[442] BLOUSTEIN, E.J. *Privacy as an aspect of human dignity: an answer to Dear Prosser*. New York University Law Rewiew vol. 39, 1964, p. 964-1007.

[443] En este sentido, CORRAL TALCIANI, H. *Configuración jurídica del derecho a la privacidad II: concepto y delimitación*. Revista chilena de derecho, vol. 27 núm. 2, Sección Estudios. 2000, p. 331-355.
Disponible en: http://dialnet.unirioja.es/servlet/articulo?codigo=2650218.

[444] WESTIN, A.F. *Privacy and Freedom*, Washington and Lee Law Review, vol. 25, num. 166. 1968.
Disponible en: http://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20/.

[445] En este sentido PIÑAR MAÑAS, J.L. "Protección de datos: origen, situación actual y retos de futuro", en *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, p. 84.

[446] PIÑAR, J.L. *¿Existe la privacidad*? Lección magistral en inauguración del Curso Académico 2008-2009. Fundación Universitaria San Pablo-CEU. CEU Ediciones, 2008.

[447] Schwartz es profesor de derecho en la Universidad de California-Berkeley y Director del Centro de Derecho y Tecnología de Berkeley.
SCHWARTZ, P.M. *Privacy and Democracy in Cyberspace*, 2.000.
Disponible en http://ssrn.com/abstract=205449.

3.2 Análisis de los modelos de la UE y de EEUU.

Desde los inicios han sido los avances tecnológicos los que han puesto el debate de la protección de datos sobre la mesa.

Sin embargo, más allá de la larga tradición democrática y de protección de los derechos y deberes del individuo, y de la doctrina generada al amparo de la *privacy* en los Estados Unidos, el sistema se ha postulado contrario a la regulación normativa y en favor de la autorregulación. El liberalismo americano no ha querido o no ha podido regular al mismo nivel que el europeo. Acerca de las razones que han llevado a esta situación ponemos de relieve las ideas analizadas por *Priscila M. Reagan*[448] así como por Leonardo Cervera[449]:

Existe una ausencia del derecho a la privacidad en la constitución estadounidense, por lo que el derecho ha de extraerse de otros principios del *Common Law*, lo cual ha generado indefinición y ha rebajado las posibilidades de las propuestas normativas. A mayor abundamiento, "el derecho a estar solo" (*to be left alone*) entra en claro conflicto con uno de los principios básicos de la constitución americana: el derecho a la libertad de expresión, reconocido en la primera enmienda constitucional.

En segundo lugar, en el sistema americano hay dos grandes grupos de derechos: los derechos civiles *(civil rights*) y las libertades públicas (*civil liberties*). No habiéndose reconocido entre los primeros podría decirse que pertenece al segundo grupo, y la realidad es que las libertades públicas ceden más fácilmente ante los derechos civiles. Junto a esto, Cervera pone de relieve dos características fundamentales de la sociedad estadounidense que no revierten en favor de la protección de datos: el poder empresarial en el entorno tecnológico (donde la protección de la privacidad supone

[448] Priscila M. Regan, *Legislating Privacy. Technology, social values and public policy*, Chapel Hill, 1995.

[449] L. Cervera Navas. "*El modelo europeo de protección de datos de carácter personal*". Cuadernos de Derecho Público 1997-2007, números 19-20. Instituto Nacional de Administración Pública, p. 131-143.
Cervera fue Administrador de la Unidad de Protección de Datos, de la Dirección General del Mercado Interior, en la Comisión Europea, y actualmente es Jefe de la Unidad de Recursos Humanos y Administración del Supervisor Europeo de Protección de Datos.

un obstáculo en el desarrollo de la tecnología) y el poco empuje electoral que tiene la privacidad para los políticos.

A todo lo aquí descrito habría que añadir las circunstancias actuales que vive el pueblo americano y que en nada favorecen el desarrollo del derecho a la privacidad: el hecho de que el pueblo se ha acostumbrado a una tecnología que ya no percibe tan peligrosa (internet, la domótica, los ordenadores personales, los *smartphones*, etc.), y el miedo a los atentados terroristas que hace permitir la pérdida de la privacidad a cambio de valores que entienden superiores como la seguridad y la defensa.

Por lo tanto, nuestros pensamientos y nuestra forma de vida difieren de la americana. Para nosotros es un derecho fundamental mientras que para los americanos no, su perspectiva es más liberal. Expertos como *Peter Hustinx* han apoyado una tercera vía, la corregulación, de modo que se creara un marco jurídico adecuado para apoyar los códigos de conducta. Tal y como reconoce *Peter Swire*[450], a pesar de que desde la década de los noventa se viene apoyando la autorregulación sin un marco legislativo, esta diferencia parece haberse reducido con el tiempo, pues en 2012 la administración Obama apoyó por vez primera una Ley de los Derechos de Privacidad[451], con idea de garantizar la seguridad de los usuarios en internet, limitando el seguimiento de las empresas a la navegación de los usuarios e intentando controlar más sus prácticas. Este proyecto de ley, que aún no ha conseguido salir adelante, tiene muchos detractores, algunos (como grupos de consumidores) por considerar que no se protege adecuadamente al consumidor debido a la falta de claridad acerca de qué tipo de información están cubiertos, así como las exenciones presentadas; otros (como empresas privadas y asociaciones de empresarios) lo rechazan ante la posibilidad de una mayor regulación y supervisión. Es difícil que este proyecto salga sin modificaciones sustanciales, pero al menos pone de manifiesto los problemas del país en la privacidad.

[450] P. Swire. "Peter Hustinx and three clichés about EU-U.S. data privacy", en Hielke Hijmans and Herke Kranenborg (Eds) *Data Protection Anno 2014: How to restore Trust?*, Cambridge. Intersentia, 2014, p 191-198.

[451] *The Consumer Privacy Bill of Rights Act of 2015*.
Para mayor información el proyecto de ley está en:
https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf

En un acto de síntesis, podríamos concretar las diferencias en cuanto al sistema de protección de datos entre ambos países en los siguientes puntos:

1.- La regulación normativa. En Europa tenemos una norma de alcance general que afecta tanto al sector público como al privado, como es actualmente la Directiva 95/46/CE y en un futuro inmediato el nuevo Reglamento General de Protección de Datos. Existe una conciencia pública de la protección de datos y un reconocimiento constitucional. En EEUU por el contrario la normativa es fundamentalmente sectorial. No hay una norma federal. La Ley Federal de 1974 (*Privacy Act*) tiene por objeto regular la obtención y el uso de la información personal dentro del sector público. No existe el reconocimiento constitucional.

2.- El enfoque. En Europa es preventivo, intentando con la regulación no llegar a los tribunales. En EEUU el sistema liberal supone un menor intervencionismo del Estado que puede ver incrementado el acceso al recurso jurisdiccional.

3.- Las sanciones. En Europa son tasadas, sin embargo en EEUU se determinan en los juzgados.

4.- La visión del ciudadano. Europa es más paternalista, y se confía en la regulación normativa que hace el Estado. En EEUU la confianza es en gran medida en la propia regulación del Mercado.

5.- La protección del ciudadano. En Europa se protege a todo ciudadano que esté en la UE. Sin embargo, en EEUU sólo a los estadounidenses.

6.- Las Autoridades de control. En Europa tenemos un Supervisor Europeo, autoridades nacionales y otras en el ámbito interno de cada país. En EEUU no hay ninguna agencia federal específica de esta materia. Son autoridades sectoriales, y es fundamentalmente la Comisión Federal de Comercio (*Federal Trade Commission*, FTC) quien asume este rol.

3.3 Los Supervisores.[452]

En Estados Unidos no existe una autoridad de protección de datos comparable a las que nos encontramos en los países de la Unión Europea. Sin embargo asigna determinadas competencias en privacidad a distintas autoridades, pues su sistema tiene un enfoque sectorial, regulando esas actividades sólo cuando hay una necesidad clara. Para muchos, este sistema es descoordinado, incompleto y asistemático.

La Ley de Privacidad de 1974[453] (*The Privacy Act of 1974*) supuso un hito en el desarrollo del derecho a la privacidad. El proyecto de ley defendido por el Senado contaba con implantar una Comisión de protección de la privacidad que supervisara a los bancos, examinara invasiones de la privacidad de las personas y prestara asesoramiento al gobierno y al sector privado; pero finalmente no se llevó a cabo. El Congreso no consideró ninguna nueva propuesta de creación de comisión hasta 1994, cuando el Senador *Paul Simon* propuso la creación de una Comisión de protección de la privacidad mediante una enmienda en la *Fair Credit Reporting Act*[454], siendo desestimada la propuesta. Posteriormente se presentaron varias más si bien nunca tuvieron una buena acogida por parte del Congreso, pero la idea de una agencia federal de la privacidad era un asunto recurrente por parte de las comisiones de estudios temporales, comisiones que abordan temas de importancia pública. Una de estas comisiones que resultó ser influyente e importante fue el Comité Asesor del Secretario en el Sistema de Datos Personales Automatizados en el Departamento de Salud, Educación y Bienestar de 1972-73, cuyas recomendaciones darían origen posteriormente a la ley federal de 1974.

---

[452] Este apartado está desarrollado casi en su totalidad sobre un artículo de *Robert Gellman*, Consultor en política de privacidad e información. Washington.
R. Gelman, "The american approach to privacy supervisión: less than the sum of its parts", en María Verónica Pérez Asinari & Pablo Palazzi (Eds) *Défis su droit à la protection de la vie privée. Challenges of privacy and data protection law*, Bruselas. Bruylant, 2008, p. 611-634.

[453] *The Privacy Act of 1974* está disponible en la web del gobierno de los EEUU: http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf.
La versión de 2015 está disponible en: http://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition.

[454] Ley de Informe Imparcial de Crédito. Disponible en: http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf

La Comisión para el estudio de protección de la privacidad creada en la *Privacy Act* recibió el cometido de hacer un seguimiento sobre la privacidad en el gobierno, estados federales y el sector privado. En 1977 publicó un informe que incluía 177 recomendaciones[455]. La primera de ellas era que debía existir un Consejo Federal de la Privacidad independiente con funciones de asesoramiento y control. El Congreso no prestó ninguna atención a dicha recomendación.

En la misma línea, también en 1977, la *Commission on Federal Paperwork* hizo más de 700 recomendaciones, siendo una de ellas en materia de privacidad la creación de una agencia federal que centralizara y coordinara la gestión de la información con poder ejecutivo. Recomendaba que la nueva agencia tuviera competencias de control, asesoramiento y cumplimiento.

La administración Clinton trabajó intensamente el tema de la organización e infraestructura administrativa en la privacidad de la información, y en 1997 el *Informaction Policy Committee* de la IITF[456] recomendó el establecimiento de una agencia independiente que no llegó a crearse, pero sí contribuyó a la última decisión de esa administración, que fue un consejero de privacidad en la Oficina de Administración y Presupuesto *(Office of Management and Budget- OMB)*.

Son muchas las agencias federales que tienen responsabilidades de política, administración, cumplimiento y otros aspectos de la privacidad, pero es difícil organizarlo porque su clasificación no responde a criterios determinados, sino que surgen de los distintos enfoques de la privacidad de las diferentes administraciones[457].

Entre ellas destaca la Comisión Federal de Comercio (*Federal Trade Commission-FTC)* por ser la que tiene otorgadas mayores competencias en materia de privacidad.

[455] *Privacy Protection Study Commission*: *Personal Privacy in an Information Society* (1977). Disponible en: https://www.ncjrs.gov/pdffiles1/Digitization/49602NCJRS.pdf.

[456] IITF.- *Information Infrastructure Task Force*

[457] Existen numerosas agencias federales, tales como: *The Office of Management and Budget(OMB), the Privacy Counselor(in the Office of Information and Regulatory Affairs at OMB), a Data Integrity Board, the Federal Trade Commission, Department of Education, Federal Communications Commission, Department of Justice, Department of Health and Human Services, Department of Commerce, Department of State, Office of Consumer Affairs and Federal Advisory Committees.*

Es un órgano regulador independiente cuyos miembros son elegidos por el Presidente y confirmados por el Senado, pero no responde ante el Presidente ni está sujeta a su supervisión. La autoridad de la FTC emana tanto de su estatuto como de la regulación práctica. Entre sus competencias está la supervisión y el cumplimiento de las leyes específicas de la privacidad[458], si bien comparte jurisdicción con otras agencias.

La FTC conoce de muchas materias relacionadas con la privacidad, y en cada una de ellas la desarrolla normativamente como considera oportuno. Cada paquete normativo es distinto e independiente de otros. También tiene capacidad para perseguir las prácticas injustas o engañosas de las actividades comerciales. Su autoridad es potencialmente amplia, si bien su jurisdicción en el sector privado no es comprensiva, ya que el mayor segmento de la economía (banca, seguros, salud, transporte y telecomunicaciones) no está sujeto a la jurisdicción de la Comisión en gran medida. Como consecuencia de ello, no puede adaptar estándares base de privacidad. La única autoridad real que tiene la Comisión es la de aplicar las leyes que el Congreso le asigna e implementar políticas de ejecución que puedan servir para delimitar las buenas o malas prácticas.

La autoridad de la Comisión sobre las prácticas injustas y engañosas se extiende a la aplicación de algunos programas de autorregulación de privacidad, incluyendo el programa de Puerto Seguro para las empresas estadounidenses que desean cumplir con los estándares de la Unión Europea. La responsabilidad sobre el cumplimiento efectivo del programa *Safe Harbour* (Puerto Seguro) es compartida con el

[458] Leyes de privacidad estadounidenses:
Fair Credit Reporting Act.. Disponible en: http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf.
*Gramm-Leach-Bliley Act (*Ley de Modernización de los Servicios Financieros*). Disponible en:* http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf.
Children´s Online Privacy Protection Act. Disponible en: http://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5
Can-Spam Act. Disponible en: http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=cea8be427690a26231dda41b8ccb5f75&ty=HTML&h=L&n=16y1.0.1.3.40&r=PART.
Do-Not-Call Implementation Act. Disponible en: http://library.clerk.house.gov/reference-files/PPL_108_010_DoNotCallImplementation.pdf.

Departamento de Transporte, siendo las competencias administrativas del Departamento de Comercio.

En los últimos años, el Congreso ha incorporado medidas en materia de supervisión sobre la privacidad en las agencias federales, si bien también alguna sobre el sector privado. En este sentido se ha creado la figura del CPO *(Chief Privacy Officer)* que asume la responsabilidad de la política de protección de datos. Como vemos es una figura similar al DPO (*Data Protection Officer)* del sistema europeo. También se requiere que cada agencia contrate un auditor independiente que supervise las actividades de privacidad, el cumplimiento y la implementación de la tecnología. Esta figura podríamos relacionarla con las auditorías que el sistema europeo viene exigiendo a los responsables del tratamiento. Un tercer elemento que se ha impuesto en el sistema americano y también tiene correlación con el europeo son las evaluaciones de impacto –PIA- (*Privacy Impact Assessments)*. Por último, y en lo que afecta al sector privado, se ha dotado de competencias a la FTC para supervisar y asegurar el cumplimiento del programa establecido en la ley *Children´s Online Privacy Protection Act* para las páginas webs que recaban datos de menores de 13 años.

Podemos decir que las aproximaciones entre los sistemas estadounidense y europeo van incrementándose. Acabamos de ver similitudes en la figura del DPO, en las auditorías independientes y en las evaluaciones de impacto.

El reciente *Consumer Privacy Bill of Rights*, de la administración Obama, de 2012, al que anteriormente nos hemos referido, representa también una aproximación de ambos sistemas. Sería un error pensar que en EEUU la privacidad no se protege, bien al contrario, como hemos ido desglosando, tiene una protección y una construcción jurisprudencial.

En cuanto a los órganos supervisores, es cierto que no existe en Estados Unidos agencia de protección de datos equivalente a las europeas, pero el debate de una agencia a nivel federal es recurrente. La FTC es el organismo que presenta más similitudes en cuanto a funciones, y tiene naturaleza de agencia independiente, y entre sus funciones está el velar por el respeto a la privacidad en las prácticas

comerciales y publicitarias de las empresas, trabajando para prevenir las prácticas engañosas, fraudulentas y desleales en el mercado, en protección del consumidor. Además, en los últimos años ha desarrollado una serie de medidas coercitivas que ofrecen hoy día ciertos elementos generales de protección en materia de protección de datos.

Tras haber analizado diferencias y similitudes de ambos modelos, podemos observar que el debate y el desarrollo normativo o de autorregulación al respecto es constante, al igual que lo es la preocupación por la mejora de los ciudadanos y muchas de las medidas que se están llevando a cabo para asegurar que los comportamientos en materia de protección de datos sean los idóneos. Teniendo en cuenta esta perspectiva en la que ambos sistemas comparten preocupación y medidas, se hace obligado, tal y como decíamos al principio, buscar los medios para llegar a un entendimiento en beneficio de las sociedades americana y europea, del progreso y del desarrollo económico.

En los últimos tiempos, al margen de la declaración de invalidez del Acuerdo de Puerto Seguro sobre el que trataremos después, los acuerdos entre la UE y EEUU han continuado. En 2010 entró en vigor (se firmó en 2003) el Acuerdo de Asistencia Judicial entre la Unión Europea y los Estados Unidos de América (*Mutual Legal Assistance Agreement*, MLAA)[459]. También recientemente han finalizado las negociaciones sobre el Acuerdo Marco sobre la Protección de Datos en el ámbito de la Cooperación Policial y Judicial *("Data Protection Umbrella Agreement"*)[460] que se estaba negociando desde el 29 de marzo de 2011, y que regula las transferencias internacionales de datos entre la UE y los EE.UU. en los casos de prevención, detención, investigación y persecución de delitos, incluido el terrorismo.

Desde el año 2013 se está negociando el Acuerdo Trasatlántico para el Comercio y la Inversión, conocido por sus siglas en inglés TTIP (*Trasatlantic Trade and Investment Partnership*), entre la UE y los EEUU. Este acuerdo tiene como objetivo crear una

[459] Disponible en: http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?redirect=true&treatyId=5441.

[460] Para mayor información acerca del *Umbrella Agreement* consultar en: http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm.

zona de libre comercio entre ambos mediante la eliminación de aranceles y armonización normativa, de modo que se impulse el comercio. Está llevándose con mucha discreción y tiene bastantes detractores entre algunos sectores sociales. En materia de protección de datos la Comisión ha reconocido que esta materia no forma parte de las negociaciones.

3.4 El acuerdo de Puerto Seguro: "*Safe Harbour*".

3.4.1 La Decisión de la CE, 2000/520/CE.[461]

La Directiva Europea 95/46/CE establece en su artículo 25 que la transferencia de datos personales a países terceros únicamente se podrá realizar cuando el país tercero garantice un nivel de protección adecuado. En su apartado 6 establece que la Comisión podrá hacer constar que ese país garantiza el nivel de protección adecuado a la vista de su legislación interna o de sus compromisos internacionales.

La Decisión de la CE, 2000/520/CE[462], de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de Puerto Seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de EE.UU, fue el resultado final de las negociaciones entre la Comisión y EEUU para cumplir con el procedimiento descrito en el apartado 6 del artículo 25 de la Directiva. Es el conocido como Acuerdo de Puerto Seguro o *Safe Harbour*[463].

[461] Sobre la regulación de la transferencia internacional de datos, ver: KUNER, C. *European data protection law*, Oxford, Oxford University Press, 2007, y *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press, 2013.

[462] Decisión 200075207CE, de 26.07.2000. DO L 215, de 25.08.2000, p.7-47. *Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.*

[463] Ver SANTOS VARA, J., *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, Centro del Derecho de las Relaciones Exteriores, Documento de trabajo del CLEER 2013/2, 2013. Disponible en: www.asser.nl/upload/documents/20130226T013310-cleer_13-2_ web.pdf.

Las negociaciones duraron dos años, pero finalmente se consiguió el acuerdo que permitía la transferencia de datos personales de un país de la Unión Europea a EEUU. De este modo las empresas que se adherían a este acuerdo se comprometían a tratar los datos conforme a los principios de Puerto Seguro establecidos en el Anexo I de la Decisión[464], los cuales se aplicaban de conformidad con la orientación que proporcionan las preguntas más frecuentes (denominadas «FAQ») publicadas por el Departamento de Comercio de Estados Unidos de América el 21 de julio de 2000, y que figuraban en el anexo II de la Decisión[465].

En cuanto al ámbito de aplicación del acuerdo, la Unión Europea -tal y como recoge en el Anexo I de la Decisión[466]- sólo reconoce como organismos jurídicos competentes de EEUU a la *Federal Trade Commission* (FTC) y el Departamento de Transportes, con arreglo a las competencias que sus propias leyes les otorgan, lo cual supone que no todos los organismos ni materias están incluidos en este Acuerdo[467].

Los principios recogidos en el Acuerdo son los siguientes:

a) Notificación.- Donde se recogen todos los deberes de información como la identificación del responsable o de la finalidad.

b) Opción.- Sería el equivalente a nuestro principio del consentimiento, ya que el interesado podrá decidir sobre la divulgación a un tercero o el tratamiento para una finalidad distinta.

c) Transferencia ulterior.- Cuando una entidad desee transferir los datos a un tercero que actúe como agente, sólo podrá hacerlo si previamente se asegura de que ese tercero suscribe los principios o es objeto de una resolución sobre su "adecuación" con arreglo a la Directiva o si firma con él un convenio por escrito para que ofrezca como mínimo idéntico nivel de protección de la vida privada que el requerido por dichos principios.

[464] Ver 462.
[465] Idem.
[466] Idem.
[467] Recordemos que el sistema de protección de la privacidad en materia de protección de datos en EEUU, y por lo tanto el de sus Agencias, es sectorial.

d) Seguridad.- Las entidades deberán tomar precauciones razonables para evitar la pérdida, mal uso, consulta no autorizada, divulgación, modificación o destrucción.

e) Integridad de los datos.- Se refiere al principio de calidad.

f) Acceso.- Supone el derecho de las personas para ejercer los derechos de acceso, rectificación, cancelación y oposición.

g) Aplicación.- Conlleva la existencia de mecanismos que garanticen la resolución de los conflictos y la verificación del cumplimiento de los principios *Safe Harbour*, con potestad para sancionar.

Toda la información acerca del procedimiento y las empresas adheridas está disponible en la página web del gobierno de EEUU[468].

Desde su aprobación en 2002 han sido más de cinco mil cuatrocientas las empresas que se han adherido al Acuerdo.

3.4.1.1 Las Autoridades de control.

En junio de 2013 *Edward Snowden*, antiguo empleado de la CIA, hizo públicos una serie de documentos secretos sobre programas de la Agencia Nacional de Seguridad de EEUU (NSA) donde trabajaba, que incluían los programas de vigilancia masiva PRISM[469]. A raíz de estas revelaciones las distintas Autoridades de control de la Unión Europea comenzaron a reaccionar, entre otras cosas porque se vieron conducidas a ello por las denuncias de los ciudadanos.

La Autoridad irlandesa, la Oficina del Comisionado de Protección de Datos de Irlanda (*The Office of the Data Protection Commissioner*), consideró inicialmente que no debía adoptar ninguna decisión, firmando de hecho en esos días, el 26 de

[468] Procedimiento y empresas adheridas al Acuerdo de Puerto Seguro. Disponible en: http://www.export.gov/safeharbor/.

[469] PRISM es un programa de vigilancia secreto de EEUU por el que se habrían vigilado a fondo las comunicaciones a través de internet (correos electrónicos, vídeo, fotos, direcciones IP, archivos…) de ciudadanos que viven fuera de EEUU y de aquellos nacionales que habían mantenido contacto con personas de fuera del país. Esta vigilancia incluía a los líderes mundiales.

junio de 2013, un memorándum de entendimiento (*Memorandum of Understanding*, MoU)[470] con la Federal Trade Commission, el cual daba mayor fuerza al Acuerdo de Puerto Seguro. También Reino Unido, a través de su Autoridad de control, the *Information Commissioner´s Office* (ICO) firmó el 6 de marzo de 2014 un memorándum de entendimiento[471] con la FTC. Los Comisionados de Protección de Datos de Berlín y Hamburgo en Alemania iniciaron a principios de 2015 dos procedimientos administrativos, respectivamente en Berlín y Bremen[472], contra dos compañías americanas que prestan servicios de nube en la Unión Europea, a efectos de suspender sus transferencias basadas en el Acuerdo de Puerto Seguro. Las autoridades alemanas han sido muy contundentes con esta materia.

3.4.1.2 La Comisión Federal de Comercio, FTC.

Haciéndonos eco de la información y los datos expuestos por la propia Comisión Europea en la Comunicación sobre el funcionamiento de Puerto Seguro de 2013[473], cuando se creó la Comisión Federal de Comercio ésta se comprometió a tramitar con carácter prioritario todos los casos presentados por las autoridades de los Estados miembros de la UE, pero dado que en los primeros diez años del sistema no se recibieron quejas, la Comisión Federal decidió buscar de oficio infracciones del Puerto Seguro en todas sus investigaciones. Desde 2009 a noviembre de 2013 (fecha del informe de la Comisión), ha puso en marcha diez acciones de ejecución que han dado lugar a órdenes de liquidación, sujetas a sanciones importantes, por declaraciones falsas en materia de defensa de la vida privada, incluido el

[470] *Memorandum* disponible en: https://www.dataprotection.ie/documents/MOU/MOU.pdf.

[471] *Memorandum* disponible en: https://www.ftc.gov/system/files/attachments/international-competition-consumer-protection-coopera-tion-agreements/140306ftc-uk-mou.pdf.

[472] Al respecto, dejamos la referencia de una nota de prensa de *Cecile Park Publishing Ltd*, de fecha 5.02.2015: http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=3201.

[473] Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE. (2013) 847 final, de 27.11.2013. Disponible en: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0847_/com_com(2013)0847_es.pdf.

incumplimiento de los principios de puerto seguro. A petición de la Comisión Federal, las entidades deben aceptar evaluaciones independientes de sus programas de protección de la vida privada, que se transmiten regularmente a la Comisión Federal, prohibiéndose la presentación de declaraciones falsas en lo que concierne a sus prácticas en materia de privacidad y a su participación en el puerto seguro. Así sucedió, por ejemplo, en las investigaciones de la Comisión Federal contra *Google, Facebook y Myspace*[474]. En 2012 Google aceptó pagar una multa de 22,5 millones de dólares para que se retirara la acusación de que había infringido una orden de consentimiento.

Tal y como acertadamente explica *Robert Gellman*[475], la Comisión Federal de Comercio ha reiterado en sus declaraciones su compromiso de tramitar con carácter prioritario todos los casos presentados por entidades autorreguladas y por los Estados miembros de la UE referentes al incumplimiento de los principios de Puerto Seguro. Pero la realidad es que las autoridades europeas de protección de datos han enviado muy pocos casos a la Comisión Federal.

La Comisión Federal de Comercio, con sus actividades de aplicación extensa y su papel en la política de privacidad, se ha establecido como una agencia creíble para la protección de la privacidad, y la Conferencia Internacional de protección de datos y privacidad ahora acepta la FTC como participante.

[474] En el período 2009-2012 la Comisión Federal de Comercio había finalizado diez medidas de ejecución relativas a compromisos de Puerto Seguro: *FTC v. Javian Karnani, and Balls of Kryptonite, LLC (2009), World Innovators, Inc. (2009), Expat Edge Partners, LLC (2009), Onyx Graphics, Inc. (2009), Directors Desk LLC (2009), Progressive Gaitways LLC (2009), Collectify LLC (2009), Google Inc. (2011), Facebook, Inc. (2011), Myspace LLC (2012).*
Para más información:
http://export.gov/build/groups/public/@eg_main/@SafeHarbour/documents/webcontent/eg_main_052211.pdf.
La mayoría de los casos sancionados se referían a problemas con entidades que se habían adherido en el pasado al marco de puerto seguro pero que, a pesar de no haber renovado su certificación anual, seguían presentándose como miembros de Puerto Seguro.

[475] Ver 452

3.4.1.3 El Parlamento y la Comisión Europea.

Desde el Parlamento se encomendó a la Comisión LIBE[476] el estudio y análisis de dichos programas de vigilancia masiva, a fin de evaluar la información, dando como resultado un informe, de fecha 11 de diciembre de 2013, que presentó una visión general de las actividades de vigilancia y las repercusiones de éstas en los derechos fundamentales de los ciudadanos europeos[477].

Las revelaciones de *Snowden* tuvieron impacto en la Comisión Europea, estableciendo acciones varias a fin de recuperar la confianza en los flujos de datos entre la UE y EE.UU. El 27 de noviembre de 2013, la Comisión emitió una Comunicación[478] dirigida al Parlamento Europeo y al Consejo sobre el funcionamiento del Puerto Seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, donde solicitaba a EEUU que restableciera la confianza en los flujos de datos entre la UE y EEUU. En este documento, tras hacer un análisis del funcionamiento del Puerto Seguro, de las incidencias presentadas en los últimos años y del funcionamiento de la FTC, la Comisión desarrolla trece recomendaciones al respecto:

- Las entidades autocertificadas deberán hacer públicas sus políticas de protección de la vida privada.

- Las políticas de protección de la vida privada que figuren en los sitios web de las entidades autocertificadas deberán incluir siempre un vínculo al sitio del Departamento de Comercio dedicado al puerto seguro, que contiene una lista de todos los miembros «actualizados» del sistema. Ello permitirá a los titulares europeos de los datos comprobar inmediatamente, sin necesidad de más búsquedas, si una entidad está adherida al marco de puerto seguro.

[476] La Comisión LIBE (Comisión de Libertades Civiles, Justicia y Asuntos de Interior) es una de las comisiones del Parlamento Europeo. Para mayor información, se puede consultar en: http://www.europarl.europa.eu/committees/es/libe/home.html#

[477] El informe LIBE está disponible en: http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-524.799&format=PDF&language=ES&secondRef=01.

[478] Disponible en: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0847_/com_com(2013)0847_es.pdf.

- Las entidades autocertificadas deberán hacer públicas las condiciones de respeto de la vida privada de todo contrato que celebren con subcontratistas, como los servicios de computación en nube.

- El sitio web del Departamento de Comercio deberá indicar claramente todas las entidades que actualmente no son miembros del sistema.

- Las políticas de protección de la vida privada que figuren en los sitios web de las entidades deberán incluir un vínculo a su proveedor de servicios de solución extrajudicial de litigios o al Panel de la UE.

- Los servicios de solución extrajudicial de litigios deberán ser asequibles y estar fácilmente disponibles.

- El Departamento de Comercio debe supervisar de manera más sistemática a los proveedores de servicios de solución extrajudicial de litigios en lo que respecta a la transparencia y la accesibilidad de la información que facilitan sobre sus procedimientos y sobre el seguimiento dado a las quejas.

- Tras la certificación o la renovación de la certificación de las entidades, conviene someter a un porcentaje de ellas a investigaciones de oficio para comprobar el cumplimiento efectivo de sus políticas de protección de la vida privada.

- Siempre que se constate un incumplimiento a raíz de una queja o una investigación, deberá someterse a la entidad a una investigación específica al cabo de un año.

- Cuando existan dudas sobre el cumplimiento por parte de una entidad, o si hay quejas pendientes, el Departamento de Comercio deberá comunicarlo a la autoridad de protección de datos de la UE competente.

- Hay que seguir investigando las afirmaciones falsas de adhesión a puerto seguro.

- Las políticas de protección de la vida privada de las entidades autocertificadas deben incluir información sobre la medida en que la legislación estadounidense permite a las autoridades públicas recoger y tratar datos transferidos al amparo de puerto seguro.

- Es importante que la excepción relativa a la seguridad nacional prevista en la Decisión de puerto seguro no se utilice más allá de lo estrictamente necesario o proporcionado.

3.4.2 El caso *Schrems.*

A lo largo de este estudio, hemos tenido la ocasión de referirnos en varias ocasiones a este caso, y es que sus implicaciones actuales hacen coherente su planteamiento desde diversos puntos de análisis. *Maximiliam Schrems* era un joven estudiante de Derecho que un día decidió ejercer su derecho de acceso ante Facebook y comprobó cómo esta empresa le envió más de mil folios, incumpliendo así la política de privacidad que supuestamente llevaba a cabo la compañía, ya que una vez recabados los datos en Europa los almacenaba en su sede en EEUU. En la documentación enviada observó que incluso las comunicaciones privadas que él había borrado seguían almacenadas y utilizadas por Facebook. Se creó la plataforma *"Europe vs Facebook"*[479].

Tras constatar el incumplimiento del Acuerdo de Puerto Seguro, *Schrems* decidió en 2011 demandar a Facebook a través de su filial en Irlanda, *Facebook Ireland Ltd* con sede en Dublín, empresa sujeta al cumplimiento de la normativa europea en protección de datos. Dicha demanda fue desestimada.

El 25 de junio de 2013 presentó una reclamación ante la Comisión de Protección de Datos de Irlanda (*Data Protection Commissioner)*[480]en la que solicitaba que se prohibiese a Facebook *Ireland* transferir sus datos personales a Estados Unidos, pues entendía que las prácticas de este país no garantizaban suficientemente la protección

[479] Disponible en: http://www.europe-v-facebook.org/ES/Objetivos/objetivos.html.
[480] Disponible en: http://www.europe-v-facebook.org/prism/facebook.pdf.

de los datos que se transferían, haciendo referencia a las revelaciones de *Edward Snowden* sobre los servicios de información de la Agencia de Seguridad Nacional estadounidense. Consideraba que había falta de transparencia de la compañía e incumplimiento de la política de privacidad.

El Comisario entendió que no estaba obligado a investigar sobre esos hechos y desestimó la reclamación alegando que las reclamaciones formuladas al respecto debían resolverse conforme a la Decisión 2000/520 en la que la Comisión había constatado que EEUU garantizaba un nivel de protección adecuado. Es obvio que la Autoridad irlandesa no deseaba involucrarse en un problema de tan alto alcance.

Frente a esta resolución, *Schrems* interpuso recurso ante el Alto Tribunal Irlandés (*High Court)* impugnando la licitud del régimen de Puerto Seguro, quien constató, a la vista de las pruebas, que si el asunto tuviera que resolverse exclusivamente bajo el derecho irlandés se debería apreciar que, dada la existencia de serias dudas de que EEUU garantice un nivel adecuado de protección de los datos personales, el Comisario habría debido llevar a cabo una investigación sobre los hechos denunciados, y que la desestimó indebidamente. Sin embargo, el asunto atañe al Derecho de la Unión, en el sentido del artículo 51 de la Carta[481], y el Tribunal entendió que se suscitaba la cuestión de si el Comisario estaba vinculado por la Decisión 2000/520 o no.

[481] Artículo 51 Carta de los Derechos Fundamentales de la Unión Europea, DO C 364, de 18.12.2000: *"Ámbito de aplicación. 1. Las disposiciones de la presente Carta están dirigidas a las instituciones y órganos de la Unión, respetando el principio de subsidiariedad, así como a los Estados miembros únicamente cuando apliquen el Derecho de la Unión. Por consiguiente, éstos respetarán los derechos, observarán los principios y promoverán su aplicación, con arreglo a sus respectivas competencias. 2. La presente Carta no crea ninguna competencia ni ninguna misión nuevas para la Comunidad ni para la Unión y no modifica las competencias y misiones definidas por los Tratados".*

3.4.2.1 La cuestión prejudicial.

El Alto Tribunal Irlandés decidió suspender el procedimiento y el 25 de julio de 2014 planteó al Tribunal de Justicia de la Unión Europea, con arreglo al artículo 267 TFUE, las siguientes cuestiones prejudiciales[482]:

"1) En el marco de la resolución de una reclamación presentada ante una autoridad independiente a la que la ley ha conferido las funciones de aplicar y ejecutar la legislación en materia de protección de datos, en la que se afirma que se están transmitiendo datos personales a un tercer país (en el caso de autos, los Estados Unidos de América) cuya legislación y práctica no prevén supuestamente una protección adecuada de la persona sobre la que versan los datos, ¿está vinculada dicha autoridad en términos absolutos por la declaración comunitaria en sentido contrario contenida en la Decisión de la Comisión de 26 de julio de 2000 (2000/520/CE), habida cuenta de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01), no obstante lo dispuesto en el artículo 25, apartado 6, de la Directiva 95/46/CE?

2) O bien, con carácter subsidiario, ¿puede y/o debe realizar el titular del cargo su propia investigación del asunto a la luz de la evolución de los hechos que ha tenido lugar desde que se publicó por vez primera la Decisión de la Comisión?"

En definitiva, si una Autoridad de control de las descritas en el artículo 28 de la Directiva 95/46/CE tiene potestad para examinar la solicitud de una persona que denuncia que el Derecho y las prácticas en vigor al transferir datos a un tercer país son contrarias a la normativa de protección de datos.

3.4.2.2 La Sentencia.[483]

La Gran Sala del Tribunal de Justicia de la Unión Europea dictó Sentencia sobre el asunto C-362/14 entre *Maximillian Schrems* y *Data Protection Commissioner*, con

[482] Disponible en: http://curia.europa.eu/juris/document/document.jsf?docid=157862&doclang=ES.
[483] Sentencia del TJUE de 6 de octubre de 2015. Asunto C-362/14. *Maximillian Schrems y Data Protection Commissioner*. Caso *Schrems / Facebook.*
Disponible en: http://curia.europa.eu/juris/document/document.jsf;?docid=169195&doclang=ES.

intervención de *Digital Rights Ireland Ltd*, el 6 de octubre de 2015, por la que declara que la interpretación del artículo 25.6 de la Directiva 95/46/CE[484] debe hacerse en el sentido de que una Decisión adoptada por la Comisión no impide que una Autoridad de control de un Estado miembro pueda investigar una solicitud presentada por una persona que alega que el Derecho y las prácticas llevadas a cabo no garantizan un nivel de protección adecuado. Asimismo declaró inválida la Decisión 2000/520/CE de la Comisión:

"1º.- El artículo 25, apartado 6, de la 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 su versión modificada por el Reglamento (CE) nº 882/2003 del Parlamento Europeo y del Consejo, de 29 de septiembre de 2003, entendido a la luz de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que una Decisión adoptada en virtud de la referida disposición, como la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46, 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, por la que la Comisión Europea constata que un tercer país garantiza un nivel de protección adecuado, no impide que una autoridad de control de un Estado miembro, a la que se refiere el artículo 28 de esa Directiva, en su versión modificada, examine la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona alega que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado.

[484] Artículo 25.6 Directiva 85/46/CE, DO L 281, de 23.11.1995: *" La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31 , que un país tercero garantiza un nivel de protección adecuado de conformidad con el aparrado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5 , a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas . Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión"*.

2º.- La Decisión 2000/520 es inválida".

Sobre las facultades de las autoridades nacionales de control a las que se refiere el artículo 28de la Directiva 95/46/CE[485], el Tribunal aclara que las disposiciones han de ser siempre interpretadas a la luz de los derechos fundamentales recogidos en la Carta, tal y como establece la jurisprudencia del TJUE[486](párrafo 38), destacando que el artículo 28.1 les encarga el cumplimiento de sus funciones con total independencia, independencia que también deriva del propio derecho primario de la Unión[487](párrafo 40). Destaca el Tribunal que esa garantía de independencia se ha establecido para reforzar la protección de las personas y de los organismos afectados por las decisiones de las propias autoridades de control, constituyendo pues un elemento esencial de la protección de datos (párrafo 41). Las autoridades de control disponen de una amplia gama de facultades, en particular recoge las facultades de investigación, como es recabar toda la información necesaria para el cumplimiento de su misión de control, facultades efectivas de intervención como la de prohibir provisional o definitivamente un tratamiento de datos, o la capacidad de comparecer en juicio (párrafo 43). Pero ciertamente entre sus facultades no está los tratamientos realizados fuera del país (p. 44). Sin embargo, la operación consistente en hacer transferir los datos desde un Estado miembro a un tercer país sí constituye un tratamiento de datos en los que tiene competencias (p.45).

Describe el Tribunal cómo el capítulo IV de la Directiva 95/46/CE (donde se incardinan los artículos 25 y 26) estableció un régimen dirigido a garantizar un control por los Estados miembros de las transferencias de datos hacia terceros países

[485] Artículo 28.1 Directiva 95/46/CE: *"Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva. Estas autoridades ejercerán las funciones que les son atribuidas con total independencia ".*

[486] Sentencias TJUE *Österreichischer Rundfunk* y otros, C-465/00, C-138/01 y C-139/01, apartado 68; *Google Spain y Google*, C-131/12, apartado 68, y *Ryneš*, C-212/13, apartado 29.

[487] Carta de los Derechos Fundamentales de la Unión Europea, DO C 364, de 18.12.2000. Artículo 8.3: *"El respeto de estas normas quedará sujeto al control de una autoridad independiente"*;
y Tratado de Funcionamiento de la Unión Europea, artículo 16.2: *"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".*

(p. 46). Como quiera que las autoridades de control están encargadas del cumplimiento de las reglas de la Unión en materia de protección de datos, entiende el Tribunal que toda autoridad nacional de control está investida de la competencia para comprobar si una transferencia de datos personales desde el Estado miembro de esa autoridad hacia un tercer país respeta las exigencias establecidas por la Directiva 95/46/CE (p. 47).

Ahora bien, la constatación de que un tercer país garantiza o no un nivel de protección adecuado pueden realizarla bien los Estados miembros o bien la Comisión (p. 50), la cual con fundamento en el artículo 25 de la Directiva 95/46/CE puede adoptar una decisión que verifique que un tercer país garantiza un nivel de protección adecuado, y en virtud del artículo 288.4 del TFUE[488] esa decisión tiene carácter obligatorio para todos los Estados miembros destinatarios y vincula por tanto a todos sus órganos en cuanto tiene el efecto de autorizar transferencias de datos personales desde los Estados miembros al tercer país al que se refiere dicha decisión (p.51), por lo que mientras la decisión no sea declarada inválida los estados miembros y sus órganos, entre ellos las autoridades de control independientes, no pueden ciertamente adoptar medidas contrarias a esa decisión (p.52).

No obstante, una decisión de la Comisión no puede impedir que las personas cuyos datos personales hayan sido o pudieran ser transferidos a un tercer país presenten a las autoridades nacionales de control una solicitud para protegerse al respecto; y una decisión tampoco puede dejar sin efecto ni limitar las facultades expresamente reconocidas a las autoridades nacionales de control (p.53). Ni el artículo 28 de la Directiva 95/46 ni el 8 de la Carta excluyen del ámbito de competencia de las autoridades nacionales el control de las transferencias de datos personales a terceros países a los que se refiera una decisión de la comisión al amparo del artículo 25 de esa Directiva (p. 54).

Por el contrario, el artículo 28 de la Directiva se aplica por su propia naturaleza a todo tratamiento de datos personales. Por tanto, incluso habiendo adoptado la Comisión una decisión en virtud del artículo 25.6, las autoridades nacionales de

[488] Artículo 288.4 TFUE: *"La decisión será obligatoria en todos sus elementos. Cuando designe destinatarios, sólo será obligatoria para éstos".*

control ante las que una persona haya presentado una solicitud de protección de sus derechos frente al tratamiento de datos que la conciernen, deben poder apreciar con toda independencia si la transferencia de esos datos cumple las exigencia establecidas por la Directiva (p. 57). Para el TJUE si esto no fuera así las personas quedarían privadas del derecho garantizado por el artículo 8 de la Carta[489] (p.58). Recuerda el Tribunal su reiterada jurisprudencia[490] según la cual la Unión es una Unión de Derecho en la que todos los actos de sus instituciones están sujetos al control de su conformidad, en particular, con los Tratados, con los principios generales del derecho y con los derechos fundamentales. Por tanto, las decisiones de la Comisión adoptadas en virtud del artículo 25.6 de la Directiva no pueden quedar excluidas de ese control (P.60).

En cuanto a la validez de la Decisión 2000/520 de la Comisión, para el Tribunal la expresión "*que un tercer país garantice un nivel de protección adecuado*" ha de equivaler al garantizado en la Unión por la Directiva 95/46/CE (p.73), siendo el tercer país el que debe garantizarlo (p.74).

Considera asimismo el TJUE que era la Comisión la obligada a apreciar el contenido de las reglas del tercer país así como la práctica seguida para asegurar el cumplimiento de las mismas (p.75). Y dado que el nivel de protección puede evolucionar, incumbe a la Comisión comprobar periódicamente la constatación del nivel de protección adecuado garantizado, y dicha comprobación debe ser obligada cuando hay indicios que generan dudas (p. 76), debiéndose tener en cuenta las circunstancias sobrevenidas tras la adopción de la decisión (p. 77).

Por lo tanto el Tribunal considera que la Comisión debiera haber llevado a cabo un control y un seguimiento del nivel de protección comprometido que no hizo.

---

[489] Carta de los Derechos Fundamentales de la Unión Europea, DO C 364, de 18.12.2000. Artículo 8: *"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".*

[490] Sentencias del TJUE Comisión y otros/*Kadi*, C-584/10 P, C-593/10 P y C-595/10 P, apartado 66; *Inuit Tapiriit Kanatami* y otros/Parlamento y Consejo, C-583/11 P, , apartado 91, y Telefónica/Comisión, C-274/12 P, apartado 56).

Analiza también la Decisión en si misma, y considera que la fiabilidad del sistema de autocertificación del Acuerdo de Puerto Seguro, donde las entidades se adhieren al sistema, existirá en tanto se establezcan mecanismos eficaces de detección y de control que permitan identificar y sancionar en la práctica las posibles infracciones de las reglas (p. 81), y que en la Decisión no se contienen constataciones suficientes sobre las medidas con las que EEUU garantiza un nivel de protección adecuado (p. 83). Además llama el Tribunal la atención acerca de la aplicación de los principios del Acuerdo exclusivamente a las entidades privadas autocertificadas, nunca a las autoridades públicas (p. 82). A esta circunstancia se añade que en los principios enumerados en el Acuerdo la aplicabilidad puede limitarse por las exigencias de seguridad, interés público y cumplimiento de la ley de EEUU (p. 84), por lo que si la legislación estadounidense establece una obligación en contra, las entidades deberán cumplirla, estén dentro o fuera del ámbito de los principios de Puerto Seguro (p.85). Ello implica que la Decisión 2000/520 reconoce la primacía de las exigencias legales de EEUU sobre los principios de Puerto Seguro, en virtud de la cual las entidades autocertificadas que reciban datos personales desde la Unión Europea están obligadas sin limitación a dejar de aplicar los principios cuando entren en conflicto con esa exigencias (p. 86). Esto supone una injerencia en el derecho fundamental a la vida privada (p.87).

Para mayor descrédito de la Decisión, el Tribunal hace expresa mención al propio análisis realizado por la Comisión en 2013[491] donde constató que las autoridades estadounidenses podían acceder a los datos personales transferidos a partir de los Estados miembros a EEUU y tratarlos de manera incompatible con las finalidades de esa transferencia, que va más allá de lo estrictamente necesario y proporcionado para la protección de la seguridad nacional. También apreció la Comisión que las personas afectadas no disponían de vías jurídicas administrativas o judiciales que les permitieran acceder a sus datos (p.90).

Sentencia el Tribunal que una normativa que permite a las autoridades públicas accedan de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada

[491] Ver 473.

garantizado por el artículo 7 de la Carta (p.94); y que una normativa que no prevea posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a sus datos personales o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta, pues la exigencia de un control jurisdiccional efectivo para garantizar el cumplimiento de las disposiciones del Derecho de la Unión es inherente a la existencia de un estado de Derecho (p.95).

En consecuencia, el Tribunal declara que el artículo 1 de la Decisión respecto de los principios que rigen el acuerdo vulnera las exigencias del artículo 25.6 de la Directiva 95/46/CE, y por lo tanto es inválido (p.98).

Respecto del artículo 3 de la Decisión 2000/520, en referencia a las competencias de las autoridades de control, declara el Tribunal que las priva de las facultades que les atribuye el artículo 28 de la Directiva 95/46/CE (p.102), y que la facultad de ejecución atribuida a la Comisión en el artículo 25.6 de esa Directiva no le confiere la competencia para restringir las facultades de las autoridades nacionales de control (p.103), por lo que la Comisión se excedió en los límites de competencias que se le atribuyeron y, por lo tanto, el artículo 3 también es inválido (p. 104).

Siendo los artículos 1 y 3 indisociables de los artículos 2 y 4 y de los anexos, la invalidez de los primeros tiene el efecto de afectar a la validez de la Decisión en su conjunto (p. 105).

3.4.2.3 Consecuencias de la Sentencia.

A nuestro juicio, el Tribunal de Justicia de la Unión Europea ha demostrado ser eficaz una vez más.

Esta sentencia ha removido los cimientos de las grandes empresas y por lo tanto de Europa y de EEUU. En el momento actual el Acuerdo de Puerto Seguro es inválido y por lo tanto no existe. Pero no es menos cierto que quienes estábamos siguiendo el caso barajábamos una alta probabilidad de que esto ocurriera. Además, la propia Comisión, el Grupo de Trabajo del Artículo 29 y el Supervisor Europeo de

Protección de Datos[492] venían advirtiendo del incumplimiento y de la necesaria modificación desde hace tiempo. Por lo tanto no ha sido una sorpresa.

A pesar de ello, las autoridades estadounidenses han cuestionado la decisión del Tribunal y han mostrado su disconformidad con la misma. La secretaria de Comercio *Penny Pritzker* dijo que Washington está "*profundamente decepcionado*" por el fallo, pues "*crea una importante incertidumbre para las empresas tanto de Estados Unidos como de la Unión Europea y pone en riesgo la economía trasatlántica digital*"[493].

Pero esta situación evidentemente no supone que no se puedan transferir ahora los datos personales a EEUU, pues las herramientas para la transferencia siguen existiendo de idéntica manera. Lo que ocurre es que hasta en tanto no se renueve el Acuerdo y exista una Decisión de la Comisión por la que ésta autorice la transferencia de datos personales al otro lado del Atlántico, dichas transferencias deberán hacerse solicitando permisos a las Autoridades de control nacionales. Soluciones alternativas también existen para no tener que transferir datos en muchas ocasiones, tal y como reconocía el propio *Schrems*, pues hay empresas que ya ofrecen la posibilidad a sus clientes de guardar sus datos en "la nube" en servidores europeos y no estadounidenses. Una solución que quizá adopten otras compañías.

Lo que sí es una realidad es que en el momento actual existe un bloqueo temporal por las grandes empresas que utilizaban el mecanismo de Puerto Seguro respecto de la transferencia de datos a los EEUU. En España siempre es posible, tal y como hacen muchas empresas, solicitar autorización a la Directora de la Agencia Española de Protección de Datos para que permita la transferencia internacional previa declaración de nivel de seguridad equiparable con la empresa en cuestión en EEUU.

[492] Dictamen del Supervisor Europeo de Protección de Datos de 20 de febrero de 2014 relativo a la Comunicación de la Comisión al Parlamento Europeo y al Consejo "Restablecer la confianza en los flujos de datos entre la UE y EEUU" y relativo a la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del Puerto Seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, en el que manifestaba abiertamente que el Acuerdo *Safe Harbour* debía ser modificado. Para mayor información, ver: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-02-20_EU_US_rebuliding_trust_EN.pdf.

[493] Declaraciones recogidas por varios medios de comunicación, entre ellos CNNEXPANSION, el 6.10.2015, disponible en: http://www.cnnexpansion.com/tecnologia/2015/10/06/europa-invalida-acuerdo-ueeu-sobre-transferencia-de-datos.

Para ello las empresas deberán presentar contratos entre exportador e importador de datos basadas en modelos contractuales tipo[494] al amparo de la Decisión 2010/87/UE de la Comisión[495].

La situación es en cierta medida desconcertante, pues las empresas no pueden parar su actividad, y en consecuencia están actuando con toda la inmediatez que el sistema permite. Entendemos que un nuevo Acuerdo de Puerto Seguro con garantías adecuadas se llevará a cabo a corto o medio plazo, pero en ese ínterin las empresas continúan y han de estar cubiertas legalmente, y ello supone actualmente elaborar Reglas Corporativas Vinculantes (CBR) o contratos con todas las partes que intervienen en el proceso de transferencia de datos en cada empresa y presentarlos a la autorización de la Directora de la Agencia.

Así pues consideramos que algunos de los efectos inmediatos que la sentencia *Schrems* va a tener son los siguientes:

1.- Reacción de las empresas que transfieren datos a los EEUU firmando acuerdos con todos los importadores de datos que deberán ser autorizados en el caso de España por la Directora de la Agencia.

2.- Ello generará una situación de confusión en estas empresas dado que deberán hacerlo en cada país de la Unión Europea en el que trabajen, debiendo someterse a normativas diferentes.

3.- Avalancha de denuncias ante las Autoridades de control nacionales.

4.- Multiplicación del trabajo en las Autoridades de control nacionales.

Frente a la creencia generalizada de la confusión que puede ocasionar esta situación, considero que ésta va a venir más por la indefinición que por el cumplimiento de la

[494] El modelo de cláusulas contractuales de la Agencia Española de Protección de Datos para las transferencias internacionales de datos entre encargado y subencargado del tratamiento están disponibles en: https://www.agpd.es/portalwebAGPD/resoluciones/autorizacion_transf/common/pdfs/MODELO-DEFINITIVO-AEPD_Contrato-encargado-subencargado-21-03-2012.pdf

[495] DECISIÓN de la Comisión de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo. DO L 39, de 12.02.2010, p. 5-18.

normativa. A saber, las multinacionales tienen infraestructura suficiente para afrontar este cambio. El seguimiento del proceso del caso *Schrems* ha sido público, por lo que estas empresas estaban preparadas y tendrán en corto plazo solventado el problema de la transferencia en cuanto sus normas o contratos sean autorizados. Ahora bien, el gran problema podría venir de la falta de armonización (que tanto se predica para la nueva normativa europea) entre las distintas Autoridades de control de la UE tanto para las exigencias en las autorizaciones de las transferencias internacionales como para la aplicación de criterios uniformes a raíz de la sentencia.

En este sentido, el Grupo de Trabajo del Artículo 29 ha hecho pública una declaración conjunta[496] sobre las primeras consecuencias que se pueden extraer a nivel europeo y nacional tras el que califican de "*histórico fallo de la Corte de Justicia de la Unión Europea*" en el caso *Maximilian Schrems* vs. Comisionado de Protección de Datos. Las Autoridades de protección de datos de la UE consideran que es absolutamente imprescindible contar con una posición sólida, colectiva y común sobre la aplicación de la sentencia.

Tal y como dice la Agencia Española de Protección de Datos en su nota de prensa al respecto de la declaración conjunta[497] "*el Grupo de Trabajo insiste en las responsabilidades compartidas entre las Autoridades de protección de datos, las Instituciones de la UE, los Estados miembros y las empresas para encontrar soluciones sostenibles para aplicar la sentencia del Tribunal. En particular, y en el contexto de la sentencia, las empresas deberían reflexionar sobre los eventuales riesgos que asumen al transferir datos y considerar la oportuna puesta en práctica de todas las soluciones legales y técnicas para mitigar esos riesgos y respetar el acervo comunitario de protección de datos*".

En línea con nuestro análisis, considera el Grupo de Trabajo que serán las Cláusulas contractuales tipo y las Normas Corporativas Vinculantes las que podrán seguir

[496] Declaración disponible en: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.

[497] Nota de prensa disponible en: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2015/notas_prensa/news/2015_10_19-ides-idphp.php.

utilizándose, si bien ello no impedirá que las Autoridades de protección de datos investiguen casos particulares y ejerzan sus poderes con el fin de proteger a las personas.

La Declaración va más allá, y dice que si a finales de enero de 2016 no se ha encontrado una solución adecuada con las autoridades estadounidenses, y en función de la evaluación de las herramientas de transferencia por parte del Grupo de Trabajo, las Autoridades de protección de datos de la UE se comprometen a adoptar todas las medidas necesarias y apropiadas, que pueden incluir acciones coordinadas de aplicación de la ley (*enforcement*).

A raíz de estas declaraciones, la propia Comisión Europea ha hecho pública el día 6 de noviembre una Comunicación[498] en la que se marca el objetivo de cerrar dicho acuerdo en tres meses.

Con base a lo que acabamos de exponer, queda constancia clara de la necesidad de una autoridad supraestatal que coordine y dicte normas armonizadas directamente ejecutables para todas las autoridades nacionales de control de la Unión Europea, y que a su vez actúe como organismo de supervisión externo a fin de verificar el cumplimiento de las futuras decisiones o acuerdos que se tomen en materia de transferencia internacional de datos personales.

[498] http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf.

4 CAPÍTULO III. Legislación y Supervisión en España.

4.1 Marco constitucional.

4.1.1 Antecedentes.

El 19 de febrero de 1900 apareció publicada en la Gaceta de Madrid la siguiente Real Orden[499]:

"Excmo. Sr: Vista la petición formulada por D. Antonio Comyn en instancia fecha 1º del corriente solicitando que en todas las oficinas del Estado, de las provincias y de los Municipios se admitan las instancias y demás documentos hechos con máquinas de escribir en los mismos términos y con los mismos efectos de los escritos o copiados a mano:

Considerando que no existe ninguna razón administrativa ni de otra índole que aconseje no admitir en las oficinas anteriormente citadas las instancias y demás documentos que en ellas se presenten hechos con máquinas de escribir, siendo más clara y fácil su lectura que muchos de los escritos a mano y cuya legalidad consiste en la autenticidad de la firma que los suscribe y no en que estén hechos precisamente con letra manuscrita.

S.M. el rey, y en su nombre la Reina Regente del Reino, han tenido a bien disponer que en todas las oficinas del Estado, provinciales y municipales, se admitan cuantas instancias y documentos se presente hechos con máquina de escribir, en los mismos términos y con iguales efectos de los escritos o copiados a mano".

[499] Gaceta de Madrid, de 19.02.1900, tomo I, p. 607.
Disponible en: https://www.boe.es/datos/pdfs/BOE//1900/050/A00607-00607.pdf.

El 23 de junio de 2007, el Boletín Oficial del Estado (la antigua Gaceta de Madrid), publicó la ley 11/2007, de 22 de junio[500], de acceso electrónico de los ciudadanos a los Servicios Públicos, en cuya Disposición Final segunda establece:

"Publicación electrónica del «Boletín Oficial del Estado». La publicación electrónica del «Boletín Oficial del Estado» tendrá el carácter y los efectos previstos en el artículo 11.2 de la presente Ley desde el 1 de enero de 2009".

En dicha fecha deja de publicarse en soporte papel "La Gaceta de Madrid".

Esta anécdota, en la que transcurre algo más de un siglo, nos acerca a la revolución que la tecnología ha supuesto en nuestras vidas, donde el crecimiento de la misma ha sido exponencial y a cuyo desarrollo España afortunadamente se ha ido incorporando, unas veces con mayor y otras con menor acierto.

Ha sido preocupación casi constante del hombre a lo largo de su historia salvaguardar su esfera íntima y privada. Ya en el siglo XVIII, las declaraciones de derechos de las revoluciones burguesas[501] fijaban unos derechos de defensa del individuo que exigían a su vez una actuación de los poderes públicos carente de intervencionismo.

Los acontecimientos acaecidos en Europa y Estados Unidos relatados en el capítulo 1 y 2 respectivamente de este estudio, fueron, al igual que para el resto de países de la Unión Europea, la base e influencia del devenir de su historia en lo que se refiere al derecho a la protección de datos, y que tiene su origen en el concepto de privacidad que paulatinamente se iría desarrollando. Así, la Declaración Universal de Derechos Humanos de la Asamblea General de las Naciones Unidas, de 10 de diciembre de 1948, reconociendo el derecho a la vida privada, a la familia, al domicilio y a la

[500] Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. BOE núm. 150, de 23.06.2007, p. 27150 a 27166.
Disponible en: http://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-12352.

[501] "La declaración de 1789, como los textos de las Colonias Inglesas que se separan de la metrópoli-Declaración de Independencia de 4 de julio de 1776, Declaración del Buen Pueblo de Virginia de 12 de julio de 1776, y más tarde las diez primeras enmiendas a la Constitución Federal de 1787, que se aprueban en 1791- son el último eslabón de una primera generación de los derechos humanos, que arrancan del siglo XVI en el marco de una preocupación de la burguesía por limitar el poder del moderno Estado Absoluto". *Historia de los Derechos Fundamentales*. Tomo II Siglo XVIII. Ed. Dykinson (2001), p.26.

correspondencia, a no ser objeto de ataques a su honra o reputación y al reconocimiento del derecho a la protección por ley contra tales injerencias[502]; el artículo 8 del Convenio para la Protección de los Derechos Humanos y Libertades Fundamentales de 1950[503] del Consejo de Europa, que recoge el derecho al respeto a la vida privada y familiar, al domicilio y a la correspondencia, y la obligación de la autoridad pública de no injerir en el derecho, salvo excepciones. También el Pacto de los Derechos Civiles y Políticos, firmado en Nueva York el 16 de diciembre de 1966 reconoce en sus artículos 17 y 19 estos derechos.[504]

El derecho a la protección de datos de carácter personal es un derecho fundamental reciente cuyo nacimiento y evolución va directamente ligado al desarrollo tecnológico, especialmente la informática, así como a la necesidad de reaccionar frente a los riesgos que esta podía suponer, si bien es cierto que aunque no en el espíritu constituyente (como veremos más adelante) su desarrollo también va ligado en ocasiones al deseo de aprovechamiento de los recursos informáticos para la Administración, como lo es el Plan Informático Nacional de 1978[505].

En España, a pesar del sistema político a comienzos de los años setenta, el Estado consciente de la existencia de esos derechos por los ciudadanos y del peligro o incertidumbre que generaba el desarrollo de la informática, dictó el 18 de febrero de 1970 una Orden del Ministerio de Justicia por la que se convocaban unas *"Jornadas de estudio sobre perfeccionamiento y modernización de los medios y métodos de la justicia"* [506] que analizaría el impacto del télex y los ordenadores en la administración de justicia. El 9 de abril del mismo año publicó una Orden del

[502] Declaración Universal de los Derechos Humanos (DUDH) de las Naciones Unidas. Asamblea General, resolución 217 A (III), de 10.12.1948. Artículo 12. Ver 3.
[503] Consejo de Europa, Convenio Europeo de Derechos Humanos, CETS Nº 5, Roma 1950.
[504] Pacto Internacional de los Derechos Civiles y Políticos. Asamblea General de las Naciones Unidas, resolución 2200 A (XXI), de 16.12.1966, Nueva York.
Artículo 17: *"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".*
Artículo 19.- *"1.- Nadie podrá ser molestado a causa de sus opiniones".*
[505] Plan Informático Nacional de 1978. BOE núm. 240, de 7.10.1978.
Disponible en: https://www.boe.es/boe/dias/1978/10/07/pdfs/A23348-23349.pdf.
[506] BOE núm. 50, de 27.02.1970.
Disponible en: https://www.boe.es/boe/dias/1970/02/27/pdfs/A03158-03158.pdf.

Ministerio de Justicia que desarrollaba normas provisionales para el télex judicial[507]; y el 12 de septiembre de 1970 dictó un Decreto de la Presidencia del Gobierno por el que se creaba la Comisión Interministerial de Informática y el Servicio Central de Informática[508], cuyo objetivo era el apoyo en la programación informática de los distintos ministerios. En este Decreto da por vez primera una definición legal de la Informática[509].

Poco antes de la promulgación de la Constitución española de 1978, se aprobó un Decreto de la Presidencia del Gobierno que creaba una Comisión interministerial para la elaboración del Plan Informático Nacional[510] cuya misión era analizar la situación que en aquél momento presentaban en España los diversos sectores[511] de la Informática y marcar unos objetivos a medio plazo definiendo una política informática que coordinara toda la acción del sector público para la mejor utilización de los recursos disponibles o que pudieran disponerse, y señalara al sector privado los criterios de la Administración, para todo lo cual debería proponer la estructura más adecuada de carácter administrativo que garantizara la adecuada ejecución.

A nivel europeo, en 1973 el Comité de Ministros del Consejo de Europa recomendó a los gobiernos de los Estados miembros tener en cuenta los abusos o mal uso de los

[507] BOE núm. 98, de 24.04.1970. Disponible en: http://www.boe.es/boe/dias/1970/04/24/pdfs/A06454-06457.pdf.

[508] BOE núm. 243, de 10.10.1970. Disponible en https://www.boe.es/boe/dias/1970/10/10/pdfs/A16662-16663.pdf.

[509] Artículo 1 Decreto de 1970: "A los efectos de la aplicación del presente Decreto se entenderá por "Informática" el conjunto de técnicas y métodos necesarios para la utilización de los equipos de proceso de datos. A los mismos, efectos se considerarán "equipos de proceso de datos" aquellas máquinas y dispositivos capaces de elaborar información registrada en forma digital, siempre que la entrada de los datos o la salida de los resultados tenga lugar sobre un soporte creado o aceptado por otras máquinas. Asimismo, se entenderá por "equipos de proceso de datos" las máquinas y dispositivos capaces de aceptar o crear dichos soportes de información o de transmitir ésta a otras unidades".

[510] Ver 505.

[511] Entiende dicho plan por sectores de la informática los de producción, adquisición, utilización y mantenimiento de máquinas y programas informáticos, su comercio de importación y exportación, la investigación y la enseñanza de la Informática, el análisis de las aplicaciones de esa tecnología y de la problemática de la transmisión de los datos, el estado de los programas de cooperación internacional y el desarrollo de la información sobre todo el fenómeno informático.

bancos de datos en el sector privado[512], y en 1974 lo hizo respecto del sector público[513].

Nuestra Carta Magna será una de las primeras en recoger la protección de los datos frente al uso de la informática, estando muy influenciada en este caso por Portugal, que fue el primer país que reconoció ese derecho fundamental en su Constitución de 1976[514].

El debate constituyente para incluir en el texto constitucional la protección frente al uso de la informática[515], tal y como acertadamente expone Pérez Luño[516], recogió tres posturas diferenciadas:

- Primera postura: la de aquellos que se posicionaron en contra de la referencia expresa a la informática por considerar, que la garantía sobre el derecho a la intimidad y al honor recogida en el apartado 1 del artículo ya era suficiente para cubrir cualquier agresión contra los derechos descritos; y además porque entendían que no era procedente "*hacer una mención expresa a la informática y no a otra serie de técnicas o medios que también pueden ir contra la intimidad personal y familiar y contra el honor de los ciudadanos"*[517]. Fue la postura adoptada por la Unión de Centro Democrático (UCD).

[512] Resolución (73) 22, de 26 de septiembre. Consejo de Ministros del Consejo de Europa. Adoptada durante la 224 reunión de los Delegados de los Ministros, relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector privado.

[513] Resolución (74) 29, de 20 de septiembre. Consejo de Ministros del Consejo de Europa. Adoptada durante la 236 reunión de los Delegados de los Ministros, respecto a la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector público.

[514] Artículo 35 Constitución portuguesa de 1976: *"Utilización de la informática 1. Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma de registros mecanográficos acerca de ellos y de la finalidad a que se destinan las informaciones y podrán exigir la rectificación de los datos, así como su actualización. 2. No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos".* Disponible en: http://www.wipo.int/wipolex/es/text.jsp?file_id=179476.

[515] Sobre la creación de nuevos derechos, SÁNCHEZ JIMÉNEZ, E. *Los derechos humanos de la tercera generación: la libertad informática*, en Informática y Derecho, núm. 4, 1994, pp. 165-175. BARRATI ESTEVE, J. *Dimensión constitucional de la limitación del uso de la informática. La protección de los datos personales*, León, 1997.

[516] PÉREZ LUÑO, A. *Informática y libertad. Comentario al artículo 18.4 de la Constitución española*. Revista de Estudios Políticos (Nueva Época), núm. 24, Noviembre-Diciembre 1981, p.31-53.

[517] Intervención del sr. Sancho Rof, en DSC, de 19.05.1978, núm. 70, p. 2526.

- Segunda postura: la de los que consideraban que había que incluir el uso de la informática, pero como garantía de todos los derechos. El texto inicialmente propuesto fue que *"La ley regulará el acopio, uso y difusión de los datos personales contenidos en los archivos o registros, susceptibles de acceso automático, con objeto de garantizar las libertades públicas y el ordenamiento constitucional*"[518]. Pero a esta propuesta el sr. Roca Junyent presentó una enmienda para ampliar la cobertura frente a posibles abusos de la informática: "*entre los límites de la informática el que se garantice el pleno ejercicio de los derechos por parte de los ciudadanos"*[519]. Este texto con su enmienda fue apoyado por Minoría Catalana, Socialistas de Cataluña y el Grupo Comunista.
- Tercera postura: pretendía que se ampliara la cobertura del derecho no sólo a la informática, sino a todos los procedimientos o medios técnicos que pudieran afectar al ejercicio de la libertad: *"Para garantizar el honor y la intimidad personal, familiar y social de los ciudadanos y el pleno ejercicio de sus derechos, la ley limitará la utilización de la informática y otros procedimientos o técnicas que puedan atentar contra los citados derechos"*[520]. Presentada mediante un voto particular del senador Zarazaga Burillo.

Finalmente, el texto aprobado quedó de la siguiente manera: *"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"*[521].

La regulación del derecho en nuestra Constitución desaprovechó una gran oportunidad para recoger como derecho fundamental la protección de los datos personales y ser pioneros en la regulación. Tal y como Pérez Luño[522] ha expuesto, son varias las críticas que pueden realizarse sobre el "*tratamiento parlamentario de*

[518] Intervención del sr. Gastón Sanz, en DSC, de 19.05.1978, núm. 70, p. 2527.
[519] Intervención del sr. Roca Junyent, en DSC, de 19.05.1978, núm. 70, p. 2527
[520] Intervención del sr. Zarazaga Burillo, en DSC, de 27.09.1978, núm. 60, p. 2981.
[521] Dictamen de la Comisión constitucional del Congreso. Boletín Oficial de las Cortes de 1.07.1978.
[522] Ver 516.

la informática". En primer lugar, si el deseo era extender la garantía frente a los abusos informáticos a todos los derechos fundamentales, hubiera sido preferible recogerlo en un artículo expreso de la Constitución, tal y como hizo la Constitución de Portugal. El incluirlo como un apartado más del artículo 18 dedicado al reconocimiento al derecho a la intimidad, *"puede dar pie a opciones hermenéuticas que dificulten la extensión de su tutela a los demás derechos y libertades fundamentales".* Por otro lado, se desarrolló una concepción negativa del derecho, ya que se establece que "*la ley limitará el uso de la informática"*, lo que presupone una postura defensiva por parte de los constituyentes, dándole relevancia a la dimensión negativa de la informática en cuanto había que limitarla. Se debió haber incluido una descripción del derecho como actuación positiva de los individuos refiriéndose al derecho de acceso el control por los ciudadanos. Además, su visión limitada a la informática dejó de lado el reconocimiento a las enormes posibilidades que la tecnología brindaba a la sociedad. Ahora bien, como reconoce el autor, una vez promulgado el derecho éste adquiere sustantividad propia: *"la Constitución, al igual que cualquier otra norma jurídica, una vez promulgada se independiza de la voluntad de sus autores y adquiere una sustantividad propia. De ahí, que la hermenéutica constitucional no deba quedarse en la razón instrumental o en la voluntad subjetiva del constituyente, sino que debe indagar todas las posibilidades que de una interpretación racional y sistemática puedan desprenderse del texto".*

Así las cosas, cuando el constituyente decide incluir la protección frente al uso de la informática en el artículo 18, en ese forma tímida en el capítulo de derechos y libertades y, concretamente en la sección 1ª "de los derechos fundamentales y de las libertades públicas", lo hace además junto a los otros derechos que "visten" la privacidad y la intimidad, lo que puede ser un mandato para mejorar las garantías de esos otros derechos, y no un derecho en sí mismo. Será con posterioridad la jurisprudencia del Tribunal Constitucional la que se encargue de dotar al derecho a la protección de datos de esencia propia, de derecho fundamental distinto y diferenciado de los otros.

Esa indecisión patente en nuestra Constitución acerca del derecho a la protección de datos se convierte en casi una negación de la realidad cuando en el listado de

competencias, ya sean exclusivas o compartidas con las Comunidades Autónomas de los artículos 148 y 149 no tiene lugar alguno. Fue un momento histórico desaprovechado para regular un derecho tan importante en nuestros días.

4.1.2 Creación del derecho fundamental del art. 18.4 de la Constitución.

4.1.2.1 Creación jurisprudencial.

El derecho fundamental a la protección de datos de carácter personal en España es de creación jurisprudencial, y ello porque ha sido el Tribunal Constitucional quien, a través de su jurisprudencia, le ha otorgado carta de naturaleza fijando los términos y el contenido del mismo.

Como hemos venido diciendo, el artículo 18.4 de la Constitución Española, además de ser impreciso, no describe tal derecho. Entendemos, a la vista de los antecedentes descritos en el apartado anterior, que el espíritu del derecho a la protección de datos debió de estar en el desarrollo de la Carta, pero lo cierto es que no se materializó.

Tres años después de la promulgación de nuestra Constitución, el Consejo de Europa aprobó el Convenio 108[523] para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, al que hemos hecho reiterada referencia en el capítulo 1. Será a partir de ese 28 de enero de 1981, día de su publicación, cuando se ponga el sistema normativo y el debate parlamentario "en la parrilla de salida". El Convenio fue ratificado por España el 27 de enero de 1984, y publicado en el BOE el 15 de noviembre de 1985.

Así pues, el Convenio 108 se convertirá en el referente normativo en la materia, que posteriormente será la base para el desarrollo de la Ley Orgánica de regulación del

[523] Consejo de Europa, Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. CETS nº 108, Estrasburgo 1981.

tratamiento automatizado de datos de carácter personal de 1992[524], y junto a la Directiva 95/46/CE serán la base para el desarrollo de la aún vigente Ley Orgánica de Protección de Datos de 1999[525], en la que se aprecia, a pesar de los muchos cambios legislativos, gran concordancia normativa con ambos instrumentos del derecho europeo.

4.1.2.2 Las sentencias del Tribunal Constitucional.

A. El reconocimiento del derecho fundamental.

Tal y como hemos venido diciendo, el que fuera reconocido en su día como *"habeas data"* adquirió carta de naturaleza gracias al desarrollo de la jurisprudencia constitucional.

La Sentencia del Tribunal Constitucional 254/1993[526] será la primera en reconocerlo.

El recurso de amparo que trae causa dicha sentencia se promueve contra la denegación presunta por parte de la Administración Pública, confirmada en vía contencioso-administrativa, de la solicitud de información relativa a los datos de carácter personal existentes en ficheros automatizados de la Administración del Estado[527]. Y ello en base al artículo 18 de la Constitución, en sus apartados 1 y 4 y a la aplicabilidad del Convenio nº 108 del Consejo de Europa que España había

[524] Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. BOE núm. 262, de 31.10.1992.

[525] Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal. BOE núm. 298, de 14.12.1999.

[526] STC 254/1993, de 20.07.1993, Sala Primera.
Recurso de Amparo nº 1827/1990.
Ponente: García-Mon y González Regueral, Fernando.
BOE núm. 197 de 18.08.1993.
Disponible en: http://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/2383.

[527] Tal y como expone el antecedente 2 de la STC 254/1993, la pretensión concreta del actor era que la Administración del estado o cualquier organismo dependiente de ella le comunicaran si disponían de ficheros automatizados donde figuraran sus datos de carácter personal y, en caso afirmativo, le indicasen la finalidad principal de los mismos, la autoridad que los controla y su residencia habitual. También solicitaba que se le comunicasen los datos existentes en dichos ficheros referidos a él de forma inteligible y sin demora.

ratificado y que sí recogía ese derecho de acceso, siendo que en la época de la solicitud aún no estaba en vigor la LORTAD.

La Audiencia había desestimado el recurso contencioso-administrativo por entender que los preceptos del Convenio no pueden ser aplicados directamente, y que tal aplicación se hallaba supeditada a la adopción en el derecho interno de las medidas necesarias. En este mismo sentido, el Tribunal Constitucional confirmó que la aplicación práctica del Convenio precisaba de una actividad interna legislativa y reglamentaria que el Estado no había aún desarrollado, además de la existencia de disposiciones administrativas referidas a la protección de datos que no hacían alusión al Convenio y la existencia de un proyecto de Ley Orgánica que ponía de manifiesto la necesidad de su promulgación para aplicar los textos.

La cuestión se centraba en determinar si la negativa de la Administración a suministrar la información solicitada vulneraba o no los derechos fundamentales a la intimidad y a la propia imagen reconocidos en los apartados 1 y 4 del artículo 18 de la CE, siendo el "nudo gordiano" el determinar si el artículo 8 del Convenio 108 era de aplicación directa o interpretativo de los derechos fundamentales, afirmando el Tribunal que es desde esa segunda perspectiva desde la que procede el análisis de la cuestión. Asevera la indiferencia que para el Tribunal supone que la norma internacional sea o no aplicable, cuanto el objeto del TC es asegurar la protección de los derechos fundamentales, tal y como expone el artículo 53.2 CE.

Para el Tribunal, con el artículo 18.4 nuestra Constitución se incorporó *"una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona",* haciendo un paralelismo con el desarrollo del resto de derechos fundamentales. *Considera que* estamos ante un instituto de garantía que es en sí mismo, un derecho o libertad fundamental, *"el derecho a la libertad frente a la potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama "la informática" "*[528].

[528] STC 254/1993 de 20.07.1993. Fundamento jurídico 6.

Así pues estima la pretensión del recurrente, en cuanto reconoce la existencia de un nuevo derecho, e intenta determinar el contenido mínimo del mismo. Para ello reconoce los dos elementos que ya venían distinguiéndose en la *privacy:* el elemento negativo y el positivo. El negativo es el que responde al enunciado literal del derecho, los límites del uso de la informática. Por el contrario, el positivo es el derecho de control sobre los datos relativos a la persona, lo que denomina *habeas data*, y ésta será la nueva incorporación jurisprudencial a la interpretación de este derecho en España.

El voto particular formulado por el Presidente del Tribunal, D. Miguel Rodríguez-Piñero y Bravo-Ferrer, contrario a la mayoría, puso en tela de juicio el fallo de la sentencia, al considerar que un Convenio no puede hacer las veces de legislación y que su omisión no habilita a la Administración o a los Tribunales a elaborar procedimientos extralegislativos. Y entendía el ponente que lo que hizo el Tribunal no era interpretar sino utilizar el convenio internacional como elemento de integración ante la demora del desarrollo legislativo.

B. El contenido.

En la Sentencia del Pleno del Tribunal Constitucional 290/2000[529], el Consejo Ejecutivo de la Generalidad así como el Parlamento de Cataluña interponen sendos recursos de inconstitucionalidad sobre algunos artículos de la LORTAD por la distribución de competencias entre el Estado y las Comunidades Autónomas, centrándose fundamentalmente en las funciones que la ley le atribuye a la Agencia Española de Protección de Datos (AEPD) y al Registro General (como órgano integrado en la Agencia) en materia de ficheros de titularidad privada radicados en el

[529] STC 290/2000, de 30.11.2000, Pleno.
Recursos de inconstitucionalidad 201-1993, 219-1993, 236-1993. 201/1993.
Promovidos por el Consejo Ejecutivo de la Generalidad de Cataluña, el Defensor del Pueblo, el Parlamento de Cataluña y por don Federico Trillo- Figueroa Conde, Comisionado por 56 Diputados del Grupo Parlamentario Popular.
Ponente: González Campos, Julio Diego.
BOE de 4.01.2001.
Disponible en: http://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/4274.

territorio de la Comunidad Autónoma[530], concretando la impugnación en los artículos 40.1 y 2 de la LORTAD.

Independientemente de que tratemos posteriormente de nuevo el reparto competencial, es necesario al menos, en el análisis de esta sentencia, hacer referencia a ello, porque en el fondo lo que se discute es el contenido del derecho fundamental a la protección de datos personales.

El Tribunal examina la "disputa competencial" partiendo de dos presupuestos: el contenido del derecho fundamental a la protección de datos de carácter personal y los rasgos generales que caracterizan a la AEPD.

En cuanto al contenido del derecho fundamental, dado que (a diferencia de la STC 254/93) cuando se pronuncia la sentencia estaba vigente la LORTAD, el Tribunal lo determina en base al propio contenido de la ley, a la jurisprudencia precedente y a la interpretación que desarrolla en la misma, configurando el derecho fundamental como "*un conjunto de derechos que el ciudadano puede ejercer frente a quienes sean titulares, públicos o privados, de ficheros de datos personales, partiendo del conocimiento de tales ficheros y de su contenido, uso y destino, por el registro de los mismos*" [531].

En cuanto al segundo presupuesto, los rasgos que caracterizan a la AEPD, tras analizar las instituciones del derecho comparado[532], y todas las competencias que son descritas en la LORTAD y en el Estatuto de la Agencia de Protección de Datos[533],

[530] STC 290/2000, de 30.11.2000.
Fundamento jurídico sexto.
[531] STC 290/2000, de 30.11.2000.
Fundamento jurídico séptimo, *in fine*.
· [532] Ley Sueca de 11.05.1973.
Disponible en: http://www.datainspektionen.se/in-english/legislation/the-credit-information-act/.
La vigente ley de protección de datos sueca es de 1.998.
Disponible en: http://www.datainspektionen.se/in-english/legislation/the-personal-data-act/.
· Ley de la República Federal de Alemania, siendo la actual de 2009.
Disponible en: http://www.gesetze-im-internet.de/englisch_bdsg/index.html.
· Ley Francesa de 6.01.1978.
Disponible en: http://www.cnil.fr/index.php?id=45.
· Ley Noruega de 8.06.1978.
Disponible en: https://lovdata.no/dokument/NL/lov/2000-04-14-31.
[533] Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos. BOE núm. 106, de 4.05.1993.

considera el Tribunal que hay un rasgo significativo de la Agencia, el carácter básicamente preventivo de sus funciones[534], y que es común a las instituciones existente en los países de nuestro entorno. Estimando pues que existe una correspondencia entre las funciones y potestades que la LORTAD ha atribuido a la Agencia y el carácter preventivo de sus actuaciones, es por lo que se justifica la atribución de sus funciones y potestades, *"para asegurar, mediante su ejercicio, que serán respetados tanto los límites al uso de la informática como la salvaguardia del derecho fundamental a la protección de datos personales en relación con todos los ficheros, ya sea de titularidad pública o privada"*[535].

En esta línea, concluye la fundamentación jurídica confirmando que las atribuciones dadas por la LORTAD a la Agencia de Protección de Datos lo hace para prevenir la violación del derecho, y dado que la garantía del mismo así como la igualdad de todos los españoles en su disfrute es el objetivo de la Agencia, sus funciones han de ejercerse en todo el territorio nacional, por lo que desestima los recursos presentados.

Es importante resaltar el voto particular formulado por Jiménez de Parga al que se adhiere Mendizábal Allende, quienes, compartiendo el fallo de la sentencia, hacen una crítica a los redactores del texto constitucional por no haber incluido de modo explícito el derecho a la libertad informática como derecho fundamental ni tampoco una cláusula abierta de derechos y libertades (que sí recogen otros textos constitucionales) que facilitarían la permanencia en el tiempo del texto constitucional. Considera además Jiménez de Parga que la piedra angular sobre la que se vertebra el derecho fundamental es el artículo 10.1 de la Constitución[536]: "*La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social".*

[534] STC 290/2000, de 30.11.2000.
Fundamento jurídico noveno, primer párrafo.
[535] STC 290/2000, de 30.11.2000.
Fundamento jurídico noveno, *in fine*.
[536] STC 290/2000, de 30.11.2000.
Voto particular de Jiménez de Paga, razonamiento tercero: *"La libertad informática, en cuanto derecho fundamental no recogido expresamente en el texto de 1978, debe tener como eje vertebrador el art. 10.1 CE, ya que es un derecho inherente a la persona… También son preceptos que facilitan la configuración de la libertad informática los contenidos en los arts. 18.1 … y 20.1 … entre otros, así como los Tratados y Acuerdos internacionales…".*

Entendemos acertada la crítica a los redactores de la Constitución en cuanto a no haber incluido una cláusula abierta de derechos y libertades que facilitara la duración en el tiempo de la Carta Magna, si bien consideramos que el derecho que se reconoce no es la "libertad informática", sino que va mucho más allá, pues la evolución del derecho fundamental a la protección de datos de carácter personal (ya plenamente dotado de contenido en el año 2000 cuando se dicta la sentencia) sobrepasa las fronteras de la libertad informática, pues el gran cambio de la normativa reguladora de la protección de datos de la LORTAD del año 1992 a la LOPD del año 1999 está precisamente en la garantía del derecho a la protección de todos los datos de carácter personal, los datos automatizados (en terminología ya pasada "informatizados") y los no automatizados.

C. El reconocimiento del derecho autónomo.

Es la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre[537], la que desarrolla el contenido del derecho a la protección de datos como derecho fundamental autónomo, diferenciado del derecho a la intimidad, además de ratificar el contenido declarado en las anteriores sentencias. Esta resolución tiene su origen en un recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo contra algunos preceptos de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal por vulneración de los artículos 18.1 y 4 y 53.1 CE. Falla el Tribunal Constitucional estimando el recurso y declarando contrarios a la Constitución y nulos algunos apartados de dichos preceptos.

La sentencia fija el contenido del derecho a la protección de datos como derecho fundamental y autónomo, diferenciado del derecho a la intimidad en tanto la función de ambos es distinta. Para el Tribunal, *"la función del derecho fundamental a la intimidad del artículo 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquél ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno de las intromisiones de terceros en contra de su*

[537] STC 292/2000, de 30.11.2000, Pleno.
Recurso de inconstitucionalidad 1463/2000.
Ponente: González Campos, Julio Diego.
BOE núm. 4, de 4.01.2001.
Disponible en: http://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/4276.

voluntad… El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos… Pero…nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quienes los poseen, y con qué fin"[538].

Reconoce la singularidad del derecho a la protección de datos y lo diferencia del derecho a la intimidad teniendo en consideración dos peculiaridades: el objeto de protección y el contenido.

- En cuanto al objeto de protección del derecho, para el Tribunal no son sólo los datos íntimos sino cualesquiera tipo de datos personales, públicos o privados, que identifiquen o permitan identificar a una persona: *"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 solo la intimidad individual…sino los datos de carácter personal".* Alcanza además la protección a aquellos datos que a pesar de ser públicos son datos de carácter personal y no escapan al poder de disposición del interesado: "*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 índoles, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo"*[539].
- El contenido ha de ser doble: además de tener una perspectiva negativa (al igual que el derecho a la intimidad) en la medida que confiere poder a su titular para prohibir que se haga uso de sus datos, también tiene una perspectiva positiva, pues el titular tiene una serie de facultades que le permiten detentar el poder sobre sus propios datos personales, pudiendo disponer de ellos e imponiendo a terceros obligaciones tales como solicitar consentimiento, informar o permitirle los derechos de acceso, rectificación y cancelación: *"... el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio*

[538] STC 292/2000, de 30.11.2000. Fundamento jurídico quinto, *in fine*.
[539] STC 292/2000, de 30.11.2000. Fundamento jurídico sexto, tercer párrafo.

> *impone a terceros deberes jurídicos, ... y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que solo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer".* Para el Tribunal existe es un poder de disposición sobre los datos personales que se concretan en el consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar los mismos[540].

El contenido descrito en la sentencia del Tribunal Constitucional 292/2000 queda corroborado, tal y como recoge la misma en su fundamento jurídico octavo, por todos los instrumentos internacionales existentes a la fecha de la sentencia de los que se hace eco, como son la Resolución 45/95 de la Asamblea General de Naciones Unidas, el Convenio 108 del Consejo de Europa, la Directiva 95/46 o la Carta de Derechos Fundamentales de la Unión Europea del año 2000.

4.1.3 Reparto de competencias en el Ordenamiento Jurídico español.

4.1.3.1 Las listas del sistema competencial.

El reparto de competencias en el sistema español no está descrito en la Constitución con exacta precisión, por lo que en ocasiones ha sido necesario acudir a la jurisprudencia para la interpretación de los límites de la competencia.

Para Garrido Falla[541] la pieza clave del llamado "Estado de las Autonomías" se encuentra en la distribución de competencias entre el Estado y las Comunidades Autónomas que establecen los artículos 148 y 149 de la Constitución.

En el derecho comparado existen varios modelos que resuelven el sistema competencial[542], si bien el sistema español articulado en la Constitución se haya

[540] STC 292/2000, de 30.11.2000.
Fundamento jurídico sexto, cuarto párrafo.
[541] GARRIDO FALLA, F. y otros: *Comentarios a la Constitución,* Madrid, 1980, pp. 1813 y ss.

encuadrado inicialmente en el sistema germánico o de doble lista, en el que la norma constitucional detalla dos listas: una de competencias exclusivas del Estado y otra de las que le podrán corresponder a los entes descentralizados.

Pero el sistema español es más complicado, y ello porque las competencias detalladas en la lista asumibles por las Comunidades Autónomas pueden ser o no asumidas por éstas (art. 18 CE)[543] o, al contrario, sus competencias pueden ser mayores de las otorgadas en dicho artículo: bien porque pueden incluir en sus Estatutos las competencias no atribuidas al Estado (art. 149.3 CE)[544]; bien porque pueden incluir las competencias legislativas que les delegue el Estado (art. 150.1 CE)[545]; o bien porque les sean transferidas facultades ejecutivas y de gestión de servicios estatales (art. 150.2 CE)[546].

Por ello, el sistema de doble lista se podría encajar, como dice Garrido Mayol[547], en un sistema nuevo flexible y abierto de "triple lista" que se estructuraría, según el

[542] Modelos de sistema competencial en el derecho comparado:
- El sistema de lista única, donde se enumeran las competencias exclusivas del Estado, correspondiendo las demás a los entes autonómicos. Es la de EEUU, propia de los estados federales.
- El sistema de lista única en el que se detallan las materias cuyas competencias se ceden a los entes autonómicos. Es la inversa a la anterior. Un ejemplo es Canadá.
- El sistema de doble lista, que implica una doble enumeración: materias atribuidas al Estado y materias atribuidas a los entes autonómicos. Es el sistema germánico.

[543] Artículo 148 Constitución Española: "*Las Comunidades autónomas podrán asumir competencias en las siguientes materias…"*

[544] Artículo 149.3 Constitución Española: *"Las materias no atribuidas expresamente al Estado por esta Constitución podrán corresponder a las Comunidades Autónomas, en virtud de sus respectivos Estatutos. La competencia sobre las materias que no se hayan asumido por los Estatutos de Autonomía corresponderá al Estado, cuyas normas prevalecerán, en caso de conflicto, sobre las de las Comunidades Autónomas en todo lo que no esté atribuido a la exclusiva competencia de éstas. El derecho estatal será, en todo caso, supletorio del derecho de las Comunidades Autónomas".*

[545] Artículo 150.1 Constitución Española: *"Las Cortes Generales, en materias de competencia estatal, podrán atribuir a todas o a alguna de las Comunidades Autónomas la facultad de dictar, para sí mismas, normas legislativas en el marco de los principios, bases y directrices fijados por una ley estatal. Sin perjuicio de la competencia de los Tribunales, en cada ley marco se establecerá la modalidad del control de las Cortes Generales sobre estas normas legislativas de las Comunidades Autónomas".*

[546] Artículo 150.2 Constitución Española: *"El Estado podrá transferir o delegar en las Comunidades Autónomas, mediante ley orgánica, facultades correspondientes a materia de titularidad estatal que por su propia naturaleza sean susceptibles de transferencia o delegación. La ley preverá en cada caso la correspondiente transferencia de medios financieros, así como las formas de control que se reserve el Estado".*

[547] GARRIDO MAYOL, V. *Sinopsis del artículo 149*. Congreso de los Diputados. 2003. Disponible en: http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=149&tipo=2.

autor en competencias exclusivas, competencias que pueden ser asumidas por las Comunidades Autónomas, y las demás competencias (que englobaría las materias omitidas o no mencionadas expresamente como exclusivas).

Esta triple lista también es descrita por Garrido Falla[548]: competencias exclusivas -aquellas en las que un ente agrupa todas las facultades posibles sobre una misma materia-; competencias compartidas –cuando unas facultades corresponden a un ente y las demás a otro-; y competencias concurrentes –cuando los dos tienen la posibilidad de concurrir con idénticas facultades en relación a una materia-[549].

El sistema descrito se sostiene en el "principio de disponibilidad", por el cual son las Comunidades Autónomas las llamadas a manifestar su voluntad de aumentar las cotas de poder a través de la asunción de competencias, ya sea a través de la reforma de su Estatuto vía Ley Orgánica, pero también a través de una Ley Orgánica del Estado de trasferencia o delegación del art. 150.2 de la Constitución. Tal y como ha señalado el Tribunal Constitucional en la sentencia 76/1983[550] *"son los Estatutos de Autonomía las normas llamadas a fijar "las competencias asumidas dentro del*

[548] GARRIDO FALLA, F. *El Desarrollo legislativo de las normas básicas y leyes marco estatales por las Comunidades Autónomas*. Revista de Administración Pública núm. 94, enero-abril 1981.

[549] Idem. Listado de competencias según Garrido Falla:

a) Competencias exclusivas: son aquéllas en las que un ente aglutina todas las facultades posibles sobre una misma materia, como ocurre en el art. 149.1 CE con las materias de relaciones internacionales, justicia, nacionalidad.

b) Competencias compartidas: cuando determinadas facultades corresponden a un ente y las restantes a otro. Aunque en estos casos podría también señalarse que lo compartido es la materia. El art. 149 CE recoge, en tal sentido, tanto la atribución de la legislación básica al Estado, correspondiendo el desarrollo normativo y la ejecución a las Comunidades Autónomas; como la atribución de la legislación al Estado, dejando exclusivamente en manos de las Comunidades autónomas la ejecución. A modo de ejemplo, según se dispone en el art. 149.1 CE: legislación sobre pesas y medidas, las bases y coordinación de la planificación general de la actividad económica, la legislación civil,.... que corresponden al Estado, entendiéndose, pues, que las restantes facultades pueden ser asumidas por las Comunidades Autónomas.

c) Competencias concurrentes: cuando los dos entes tienen la posibilidad de concurrir con idénticas facultades a la regulación de una materia. Sería un supuesto aplicable a la cultura (art. 149.2 CE), donde existe una concurrencia de objetivos "ordenada a la preservación y estímulo de los valores culturales propios del cuerpo social desde la instancia pública correspondiente" y en la que las competencias atribuibles a las Comunidades Autónomas no resultan incompatibles con la misión del Estado de facilitar la comunicación entre ellas, ni con la consideración de la labor cultural como un deber y atribución esencial".

[550] STC 76/1983, de 5 de agosto, Pleno.
Recursos previos de inconstitucionalidad núm. 311, 313, 314, 315 y 316/82, acumulados RI-25.
Ponente: Gloria Begué Cantón.
BOE de 18.08.1983.

marco establecido en la Constitución". El sistema competencial se articula, pues, mediante la Constitución y los Estatutos".

4.1.3.2 Competencias legislativas y de ejecución.

No es difícil de intuir que la protección de datos (que como ya hemos podido ver no aparece siquiera recogida como derecho en nuestra Constitución), no iba a formar parte de las listas de competencias exclusivas del Estado recogidas en el artículo 149 CE, ni de las que podrían asumir las Comunidades Autónomas por el artículo 148 CE. No aparece, no existe para el constituyente, y no porque no conozca de su existencia, que la conoce, sino por una falta de interés ante una materia que pensamos no se le antojaba importante o ante la que presentaba un miedo a lo desconocido. De igual modo tampoco aparece referencia alguna en los Estatutos de Autonomía hasta las reformas posteriores a las sentencias del Tribunal Constitucional 290/2000 y 292/2000, a las que ya hemos hecho referencia.

La justificación constitucional de la competencia del Estado en materia legislativa para aprobar normas relacionadas con la protección de datos nacen, tal y como expone Troncoso Reigada[551] del propio artículo 18.4 del texto constitucional, y ello por el reconocimiento como derecho fundamental que le hace estar sometido a la reserva de ley orgánica, tal y como establecen los artículos 53.1[552] y 81[553] de la Constitución, así como por la atribución al Estado de la competencia exclusiva sobre la *"regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes*

[551] TRONCOSO REIGADA, A. *La distribución competencial entre el Estado y las Comunidades Autónomas en protección de datos personales.* Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas, ISSN 1699-7026, Nº. 1, 2005 (Ejemplar dedicado a: Los derechos fundamentales y las nuevas tecnologías), p. 114.

[552] Artículo 53.1 Constitución Española: *"Los derechos y libertades reconocidos en el Capítulo segundo del presente Título vinculan a todos los poderes públicos. Sólo por ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades, que se tutelarán de acuerdo con lo previsto en el artículo 161.1 a)".*

[553] Artículo 81 Constitución Española: *"1. Son leyes orgánicas las relativas al desarrollo de los derechos fundamentales y de las libertades públicas, las que aprueben los Estatutos de Autonomía y el régimen electoral general y las demás previstas en la Constitución. 2. La aprobación, modificación o derogación de las leyes orgánicas exigirá mayoría absoluta del Congreso, en una votación final sobre el conjunto del proyecto".*

constitucionales" recogida en el artículo 149.1.1 de la Constitución. Será pues el artículo 18.4 de la Constitución española el título competencial para dictar la LORTAD y la LOPD.

El hecho de que la competencia para legislar materias básicas del ejercicio del derecho fundamental a la protección de datos corresponda al Estado español es algo que aún no ha sido discutido, ni tan siquiera en el recurso de inconstitucionalidad[554] promovido por la Generalidad en el que pretendía se declarasen inconstitucionales los preceptos de la Ley Orgánica de Protección de Datos que le atribuían a la Agencia Española de Protección de Datos la competencia exclusiva sobre los ficheros privados. Este principio supone que las Comunidades Autónomas pueden también legislar, pero siempre y cuando no se modifiquen las condiciones establecidas en la normativa básica.

La primera ley que desarrolla normativa sobre protección de datos en España es la Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, conocida como LORTAD[555]. En el Título VI de la ley se creó la Agencia de Protección de Datos, un ente de Derecho Público con personalidad jurídica propia y plena capacidad pública y privada, con capacidad para ejercer sus funciones en todo el territorio nacional.

Pero también prevé la ley en su artículo 40 la creación de órganos autonómicos que desarrollen parte de las funciones de la Agencia estatal: *"1. Las funciones de la Agencia de Protección de Datos reguladas en el artículo 36, a excepción de las mencionadas en los apartados j), k) y l) y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 45 y 48, en relación con sus específicas competencias, serán ejercidas, cuando afecten a ficheros automatizados de datos de carácter personal creados o gestionados por las Comunidades Autónomas, por los órganos correspondientes de cada Comunidad, a los que se garantizará plena independencia y objetividad en el ejercicio de su cometido.*

[554] STC 290/2000, fundamento jurídico décimo. Ver 529.
[555] Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. BOE núm. 262, de 31.10.1992.

2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros públicos para el ejercicio de las competencias que se les reconoce sobre los mismos, respecto de los archivos informatizados de datos personales cuyos titulares sean los órganos de las respectivas Comunidades Autónomas o de sus Territorios Históricos".

Siguiendo a Troncoso Reigada, la redacción de este artículo suponía el otorgamiento de competencias no legislativas sino puramente ejecutivas, para las que no existía título competencial, a un organismo estatal, ya que la Agencia de Protección de Datos española tendría el control exclusivo sobre los ficheros privados de las Comunidades Autónomas así como de los ficheros de los Ayuntamientos. La LOPD ha mantenido casi íntegro ese reparto competencial, salvo en materia de ficheros de entes locales, cuya competencia han asumido las agencias autonómicas.

Con base en este artículo de la LORTAD y posteriormente de la LOPD, el Estado se reserva la competencia de ejecución administrativa sobre los ficheros privados, pero *"el problema reside principalmente en la habilitación constitucional para que el Estado se reserve la competencia de ejecución administrativa de la legislación de protección de datos personales sobre los ficheros privados. … El alcance del art. 149.1.1 CE es esencialmente normativo… ya que estamos hablando de la regulación de las condiciones básicas… La regulación de las condiciones básicas no puede extenderse de ninguna manera a la actividad ejecutiva de policía administrativa ni a las normas organizativas que atribuyen funciones a la Agencia Española de Protección de Datos"*[556].

Siguiendo al autor, deberemos acudir al artículo 149.3 CE para buscar la habilitación constitucional de la competencia de ejecución en materia de protección de datos, por la que "*las materias no atribuidas expresamente al Estado por esta Constitución podrán corresponder a las Comunidades Autónomas en virtud de sus respectivos Estatutos. La competencia sobre las materias que no se hayan asumido por los Estatutos de Autonomía corresponderá al Estado, cuyas normas prevalecerán, en caso de conflicto, sobre las de las Comunidades Autónomas en todo lo que no esté*

[556] TRONCOSO REIGADA. Ver 551, p.115.

atribuido a la exclusiva competencia de éstas". Por tanto, si es el Estado el que ha legislado sobre esta materia podrá reservársela en tanto no la regulen las Comunidades Autónomas. A sensu contrario, si las Comunidades Autónomas reforman sus Estatutos e incluyen las competencias de ejecución en materia de protección de datos, serán éstas las que las ostenten.

Por lo tanto, constatar que el título competencial lo tiene el Estado necesita de otra argumentación adicional que la complemente, y ésta la encuentra Troncoso en el artículo 149.1 de la Constitución[557], entendiendo que el legislador puede atribuir esas funciones de control a la Agencia Española de Protección de Datos *"para preservar la igualdad de los españoles en la protección de sus datos personales, creando, de esta forma, condiciones institucionales que permitan excluir ejecuciones plurales y divergentes por las diferentes Comunidades Autónomas",* argumentación utilizada en la propia Exposición de Motivos de la LORTAD así como en el fundamento de derecho decimocuarto de la STC 290/2000[558].

Es precisamente esta sentencia, la STC 290/2000, un hito importante en el reparto competencial sobre los ficheros privados en materia de protección de datos[559] donde, tal y como hemos comentado, en ningún momento se cuestionó la validez del título competencial del Estado para dictar la LORTAD, ni tampoco se impugnó la creación de la Agencia de Protección de Datos. Tan sólo se discutieron las potestades de ejecución atribuidas a las Comunidades Autónomas donde, tal y como acabamos de ver, se limitaba su ejercicio a los ficheros creados o gestionados por dichos entes, así como la creación y mantenimiento de registros de ficheros públicos para el ejercicio de las competencias que se les reconocen sobre los mismos. Argumentaban los

[557] Artículo 149.1 Constitución Española: *"El Estado tiene competencia exclusiva sobre las siguientes materias: 1ª. La regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales".*

[558] STC 290/2000, fundamento de derecho decimocuarto: *"A este fin la LORTAD ha atribuido a la Agencia de Protección de Datos diversas funciones y potestades, de información, inspección y sanción, para prevenir las violaciones de los derechos fundamentales antes mencionados. Y dado que la garantía de estos derechos, así como la relativa a la igualdad de todos los españoles en su disfrute es el objetivo que guía la actuación de la Agencia de Protección de Datos, es claro que las funciones y potestades de este órgano han de ejercerse cualquiera que sea el lugar del territorio nacional donde se encuentren los ficheros automatizados conteniendo datos de carácter personal y sean quienes sean los responsables de tales ficheros".*

[559] Ver 529.

recurrentes[560] que la protección de datos no es una materia en si misma considerada, sino que es instrumental para el ejercicio de competencias de distintas materias, motivo por el cual, según ellos, no existía previsión constitucional ni estatutaria en materia de protección de datos. Entendían que las competencias de ejecución y tutela administrativa de la LORTAD sobre ficheros privados debían ser ejercidas por la Administración estatal o autonómica que tuviera la competencia en esa materia.

A raíz de esta argumentación que incide sobre el concepto del derecho de la protección de datos es por lo que el Tribunal Constitucional dictó una amplia sentencia en la que recogía los términos del contenido de este derecho, llevando al desistimiento del recurso planteado.

Así pues, y a modo de conclusión, la habilitación constitucional para legislar en materia de protección de datos la tiene el Estado en virtud del art. 18.4 de la Constitución por ser un derecho fundamental, y la habilitación constitucional en materia de ejecución administrativa sobre los ficheros de titularidad privada por la previsión establecida en el art. 149.1 y 3 de la Constitución Española. La competencia sobre ejecución administrativa sobre ficheros de titularidad pública la tendrán las Comunidades Autónomas siempre y cuando así lo recojan en sus Estatutos y tengan la previsión normativa necesaria para hacer frente a ello, y en tanto no la realicen será la Agencia Española de Protección de Datos la competente.

4.2 La normativa española.

El desarrollo normativo del derecho a la protección de datos de carácter personal al que el legislador español estaba obligado en virtud del mandato constitucional así como de la adhesión al Convenio 108 del Consejo de Europa, tiene en España tres hitos (con sus tres correspondientes normas) fundamentales:

1. La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD)[561];

2. La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[562] (LOPD);

3. El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal[563].

4.2.1 La LORTAD.

La LORTAD constituye una novedosa ley en protección de datos que posicionó a España como uno de los países con una legislación más completa en esta materia, aunque también más rígida. Recogía los principios del Convenio 108 del Consejo de Europa y además se hizo eco de la Directiva 95/46/CE, que si bien tardaría tres años más en aprobarse llevó varios años su preparación. Como dice Piñar Mañas "*supuso un hito en el reconocimiento del derecho a la protección de datos y sentó las bases del que es sin duda uno de los modelos europeos más garantistas y respetuosos con los derechos de las personas*"[564].

Para el desarrollo de la ley, tal y como aporta el Libro Verde de la LORTAD[565] fueron muchos los preceptos y leyes nacionales tenidas en cuenta[566], así como los

[561] Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. BOE núm. 262, de 31.10.1992.
Disponible en: https://www.boe.es/boe/dias/1992/10/31/pdfs/A37037-37045.pdf.

[562] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
BOE núm. 298, de 14.12.1999.
Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750.

[563] 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.
BOE núm. 17, de 19.01.2008.
Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2008-979.

[564] PIÑAR MAÑAS, J.L. *Protección de datos: origen, situación actual y retos de futuro*. Fundación Coloquio Jurídico Europeo. 2009, p.18. Teniendo sus consideraciones como referente un trabajo del mismo autor: "Estudio Introductoria. El derecho fundamental a la protección de datos personales.", en PIÑAR y CANALES, *Legislación de Protección de Datos*, p. 31 y ss.

[565] Libro Verde de la Protección de Datos Personales. Secretaría General del Congreso de los Diputados. BODG Congreso, Serie A, núm. 59, de 24 de julio de 1991.

Convenios internacionales ratificados por España en ese momento[567]. Pero desde nuestro punto de vista son de destacar las iniciativas parlamentarias para que el derecho a la protección de datos se regulara, iniciativas incluso anteriores a la ratificación del Convenio 108, siendo ello indicativo de una sociedad en progreso y preocupada por este derecho.

En julio de 1980, Manuel Fraga formuló una pregunta al Gobierno sobre la necesidad de un proyecto de ley de protección de datos o de Ordenación y Control del uso de la informática[568] que fue contestada por el entonces Ministro Rafael Arias Salgado en el que ya reconocía que el gobierno estaba estudiando el tema y que el proyecto de ley que se enviaría en desarrollo del artículo 18.4 CE habría de tener en cuenta *"la regulación limitativa de los ordenadores, adoptando, posiblemente, el sistema de la autorización administrativa para la explotación de ficheros informatizados que*

[566] Por orden cronológico:

- Constitución Española de 1978;
- Ley 9/1968, de 5 de abril, sobre secretos oficiales (BOE núm. 84, de 6.04.1968) ;
- Decreto 242/1969, de 20 de febrero, por el que se desarrollan las disposiciones de la ley 9/1968, de 5 de abril sobre secretos oficiales (BOE núm. 84, de 6.04.1968);
- Ley 48/ 1978, de 6 de diciembre, de protección jurisdiccional de los derechos fundamentales de la persona (BOE núm. 311, de 29.12.1978);
- Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (BOE núm. 115, de 14.05. 1982);
- Orden de 30 de julio de 1982 sobre limitación de acceso a la información contenida en las bases de datos fiscales (BOE núm. 190, de 10.08.1982);
- Ley Orgánica 3/1985, de 29 de mayo, sobre modificación de la Ley Orgánica 1/1982, de 5 de mayo sobre protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen (BOE núm. 129, de 30.05.1985);
- Ley Orgánica 3/1986, de 14 de abril, de medidas especiales den materia de salud pública (BOE núm. 102, de 29.04.1986);
- Ley 14/1986, de 25 de abril, general de sanidad (BOE núm. 102, de 29.04.1986);
- Real Decreto Legislativo 1091/1988, de 23 de septiembre, por el que se aprueba el texto refundido de la Ley general presupuestaria (BOE núm. 234, de 29.09.1988);
- Ley 12/1989; de 9 de mayo, de la función estadística pública (BOE núm. 112, de 11.05.1989);
- Ley 17/1989, de 19 de julio, reguladora del régimen del personal militar profesional (BOE núm. 172, de 20.07.1989) y
- Ley 25/1990, de 20 de diciembre, del medicamento (BOE núm. 306, de 22.12.1990).

[567] Convenios internacionales:

· Instrumento de ratificación de 26.09.1979, del Convenio de 4 de noviembre de 1950 para la protección de los derechos humanos y de las libertades fundamentales, enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente (artículo 8.2) (BOE núm. 243, de 10.10.1979) e

· Instrumento de ratificación de 7.01.1984 del Convenio de 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Hecho en Estrasburgo (BOE núm. 274, de 15.11.1985).

[568] BOCG de 24.07.1980, serie F, núm. 1024-I.

contengan datos personales, o bien los datos son personales, pero susceptibles de ser puestos en relación con una persona, es decir, los datos personalizados", reconociéndole a la persona el *"derecho de acceso a la información contenido en registros automatizados, derecho a exigir la rectificación de los datos inexactos, derecho a que los datos sean usados de conformidad con el fin para el cual fueron recogidos, derecho a exigir la actualización y, en su día, la cancelación de los datos".* Una visión avanzada de la realidad de la que nuestros políticos eran ya fieles conocedores en 1980.

Con posterioridad, en 1984, el Grupo Parlamentario Popular presentó una proposición no de ley relativa a la remisión a las Cortes de un proyecto de ley orgánica sobre Bases de Datos y protección a la intimidad en la que reconoce los derechos de acceso, rectificación y cancelación de las personas. En 1987, este mismo grupo político remite una Proposición de Ley de Protección al honor y a la intimidad de las personas frente a la utilización de las bases de datos que fue rechazada[569] que a nuestro juicio resulta destacable en cuanto que en su articulado además de contener una terminología muy similar a la actual[570], dedica un capítulo a la Inspección de protección de datos, creando la figura del Inspector de Protección de Datos también en términos equivalentes a las autoridades de control actuales[571]. En 1988, el Grupo Parlamentario Mixto- Agrupación IU-EC presentó también una Proposición de ley de Protección de los derechos y libertades en relación con el uso de la informática y las telecomunicaciones[572] mucho más detallado que el anterior y que igualmente fue rechazada. En este texto se preveía la creación de un organismo muy parecido en su descripción y competencias a la Agencia de Protección de Datos, denominado Comisión Nacional para la telemática y la protección de los derechos y libertades, cuya función era *"velar por la aplicación de esta ley, con especial atención a la*

[569] BOCG de 27.04.1987, serie B, núm. 68-I.

[570] Define lo que son datos personales, archivo o fichero automatizado, tratamiento automatizado, persona registrada o responsable del archivo (artículo segundo).

[571] Artículo noveno: *"1.- Las Cortes Generales elegirán, a propuesta del Gobierno, un Inspector de Protección de Datos por un periodo de cinco años. 2.- Corresponde al Inspector de Protección de Datos el velar por el cumplimiento de las Disposiciones de esta Le, garantizando el respeto de sus previsiones en el ámbito de la Administraciones Públicas. 3.- Anualmente, el Inspector de Protección de datos elevará una Memoria a las Cortes Generales y propondrá la adopción de las medidas que estime precisas para asegurar los objetivos de la presente Ley".*

[572] BOCG de 23.06.1988, serie B, núm. 120-I.

garantía de los derechos de los ciudadanos. Para el ejercicio de sus competencias… detentará la potestad reglamentaria e inspectora"[573], haciendo además referencia al carácter de independencia de dicho órgano[574]. El Grupo Parlamentario IU Iniciativa per Catalunya persistió en su idea y a finales de 1989 volvió a presentar otra Proposición de Ley Orgánica sobre protección de los derechos y libertades en relación con el uso de la informática y las telecomunicaciones[575].

En cuanto al cumplimiento debido por el gobierno de legislar en protección de datos como consecuencia de la adhesión al Convenio 108, el Grupo Parlamentario Mixto presentó en 1986 una proposición no de ley relativa al cumplimiento del Convenio 108 respecto del tratamiento automatizado de datos de carácter personal[576], proposición que fue desestimada.

También fueron varias las preguntas que se formularon por algunos diputados al Gobierno sobre si el ejecutivo estaba preparando alguna norma al respecto.[577]

Pero a pesar de la presión de los grupos parlamentarios en la oposición en cada momento, fue realmente la incorporación de España al espacio *Schengen*[578] la que precipitó la aprobación de la norma, cuya adhesión se produjo el 25 de junio de 1991[579], pues el Convenio de *Schengen* obligaba a los estados firmantes a desarrollar

[573] Artículos 19 a 25 de la Proposición de Ley.

[574] Artículo 23 de la Proposición de Ley: "En el ejercicio de sus atribuciones, los miembros de la Comisión Nacional son plenamente independientes y no están sometidos a ninguna Autoridad".

[575] BOCG de 22.12.1989, serie B, núm. 12-I.

[576] BOCG de 4.12.1986, serie D, núm. 20.

[577] Pregunta formulada por un diputado del CDS: *"Tiene el ejecutivo elaborada alguna norma amparando al ciudadano en el sentido de poder constatar los datos computarizados sobre su personal, para su modificación si no son ciertos, o supresión si atentas al derecho de su intimidad?*. BOCG de 17.03.1988, serie D, núm. 162.
Pregunta formulada por un diputado de Coalición Popular: *"Piensa el Gobierno enviar un proyecto legislativo a las cortes en cumplimiento del artículo 18.4 de la Constitución que limite el uso de la informática para garantizar el honor y la intimidad personal y familiar? En caso afirmativo, ¿para cuándo lo tiene previsto?*. BOCG de 13.09.1988, serie D, núm. 216.
Pregunta formulada por un grupo del PSOE: *"Para cuándo tiene el Gobierno prevista la elaboración de un proyecto que regule el mandato del artículo 18.4 de la Constitución?*". BOCG de 12.12.1990, núm. 76.

[578] Acuerdo de Adhesión del Reino de España al Convenio de Aplicación del Acuerdo de *Schengen*. Instrumento de ratificación de 23 de julio de 1993. BOE núm. 81, de 5.04.1994. Corrección de erratas en BOE núm. 85, de 9.04.1994.

[579] Pregunta escrita formulada por la diputada Loyola de Palacio al Gobierno (BOCG de 28.01.1991, serie D, núm. 148): Medidas adoptadas por el Gobierno para que, en la incorporación al Acuerdo de *Schengen*, que establece un sistema de información interpolicial automatizado, esté preparada nuestra Administración, adaptada nuestra legislación, protegidos los derechos y libertades de los

las disposiciones nacionales necesarias que garantizaran un nivel de protección de los datos de carácter personal equivalente al del Convenio 108, estableciendo como último plazo el de la entrada en vigor del Convenio de *Schengen*.

En cuanto a la influencia de la regulación internacional, además del Convenio 108 del Consejo de Europa, fueron tenidos en cuenta otros textos como las Directrices relativas a la protección de la intimidad de la circulación transfronteriza de datos personales de la OCDE[580] y la Resolución 45/95 de la Asamblea General de Naciones Unidas[581], de 14 de diciembre de 1990, por la que se establecen las directrices de protección de datos.

Así las cosas, y con los numerosos antecedentes obrantes en 1992 fundamentalmente en el derecho comparado y en la Comunidad internacional, se aprobó una ley de protección de datos muy completa y que fue modelo para las que vinieron después en otros países. Su principal diferencia con la que hoy está en vigor en España estaba en el ámbito de aplicación, pues sólo se aplicaba a los ficheros automatizados, ya que su objeto era el desarrollo del artículo 18.4 CE en cuanto a la limitación del uso de la informática.

La LORTAD tuvo un gran desarrollo reglamentario, dando así origen al Real Decreto 428/1993, de 26 de marzo, por el que se aprobó el Estatuto de la Agencia de Protección de Datos[582]; el Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal[583], y el Real Decreto 994/1999[584], de 11 de junio, por el que se aprueba el Reglamento de

ciudadanos, especialmente en relación con el uso de la informática, y para que se salvaguarden nuestras especiales relaciones con Iberoamérica.

[580] Directrices de la OCDE .Disponible en: http://www.oecd.org/sti/ieconomy/15590267.pdf.

[581] Resolución 45/95 de Naciones Unidas. Disponible en: http://www.un.org/es/comun/docs/?symbol=%20A/RES/45/95&Lang=S.

[582] BOE núm. 106, de 4.05.1993.

[583] BOE núm. 147, de 21.06.1994.

[584] BOE núm. 151, de 25.06.1999.

medidas de seguridad. Este último ha estado vigente[585] hasta el año 2007 cuando se aprobó el RD 1720/2007, Reglamento de desarrollo de la LOPD.

El Título VI de la ley es dedicado a la Agencia de Protección de Datos, un órgano especializado, creado para asegurar la máxima eficacia de las disposiciones, independiente y al que atribuye el estatuto de Ente público[586]. Dispone también la creación de órganos en las Comunidades Autónomas, cuestión que más tarde abordaremos.

Bajo la vigencia de esta ley, la Agencia elaboró una serie de Instrucciones de materias específicas que si bien no eran vinculantes, sí servían y siguen sirviendo como criterios interpretativos[587].

4.2.2 La LOPD.

Con la nueva Directiva de protección de datos de 1995 se daba un plazo de transposición a los Estados miembros de tres años[588], el cual finalizaría el 23 de

[585] Real Decreto 195/2000, de 11 de febrero, por el que se establece el plazo para implantar las medidas de seguridad de los ficheros automatizados previstas por el Reglamento aprobado por el Real Decreto 994/1999, de 11 de junio. BOE núm. 49, de 26.02.2000.

[586] Dice la Exposición de Motivos de la LORTAD, en su punto 5: *"Para asegurar la máxima eficacia de sus disposiciones, la Ley encomienda el control de su aplicación a un órgano independiente, al que atribuye el estatuto de Ente público en los términos del artículo 6.5 de la Ley General Presupuestaria. A tal efecto la Ley configura un órgano especializado, denominado Agencia de Protección de Datos, a cuyo frente sitúa un Directo".*

[587] Instrucciones de la AEPD durante la vigencia de la LORTAD:

- Instrucción 1/1998, de 19 de enero, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.
- Instrucción 2/1996, de 1 de marzo, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo.
- Instrucción 1/1996, de 1 de marzo, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.
- Instrucción 2/1995, de 4 de mayo, 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 1/1995, de 1 de marzo, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito.

[588] Directiva 95/46/CE Disposición Final, artículo 32, apartado 1: *"Los Estados miembros adoptarán las disposiciones legales… a más tardar al final de un período de tres años a partir de su adopción".*

noviembre de 1998 y en casos muy concretos, como la adaptación de ficheros manuales, hasta doce años[589].

El texto presentado por el Gobierno para transponer la Directiva era una adaptación, de la LORTAD sin pretender una nueva ley, pero el elevado número de enmiendas (ciento catorce) provocó la redacción de una nueva norma, lo que según muchos fue la causa de la más que criticada ausencia de exposición de motivos.

Novedades.

La novedad más relevante de la LOPD[590] respecto de la LORTAD es sin lugar a dudas su ámbito de aplicación, ya que (siguiendo lo establecido en la Directiva) se aplicaría tanto a ficheros automatizados como no automatizados[591].

Algunos otros aspectos que destacan en el la ley de 1999 y que suponen un cambio respecto a la de 1992 son los siguientes:

- El ámbito geográfico de la norma[592], pues la LOPD no sólo afecta a los tratamientos realizados en España por un responsable establecido en España, sino también cuando no estando establecido en territorio español le sea de aplicación la legislación española en aplicación del derecho internacional público. Además le será de aplicación cuando aun no estando el responsable situado en territorio español o de la Unión Europea se utilicen para el tratamiento medios ubicados en España, salvo que sean utilizados exclusivamente con fines de tránsito.

- El número de ficheros que pasan a estar fuera del ámbito de aplicación de la normativa pasa de cinco a tres[593].

[589] Directiva 95/46/CE Disposición Final, artículo 32, apartado 2, segundo párrafo: *"No obstante lo dispuesto en el párrafo primero, los Estados miembros podrán establecer que el tratamiento de datos que ya se encuentren incluidos en ficheros manuales en la fecha de entrada en vigor de las disposiciones nacionales adoptadas en aplicación de la presente Directiva, deba ajustarse a lo dispuesto en los artículos 6,7 y 8 en un plazo de doce años a partir de la adopción de la misma".*

[590] Sobre la LOPD, ANTONIO TRONCOSO REIGADA (Dir.). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*. Cívitas, Madrid, 2010.

[591] Artículo 2, apartado 1 LOPD.

[592] Ídem.

[593] Artículo 2.2 LOPD.

- Se incrementa también el número de definiciones[594] de la ley, teniendo especial relevancia la inclusión del consentimiento, de fuentes accesibles al público, de cesión o comunicación de datos y del encargado del tratamiento.

- En cuanto al consentimiento se recogen nuevas excepciones[595].

- Se incorpora el principio de finalidad, que deberá ser determinada, explícita y legítima para la que se hayan obtenido, prohibiendo utilizar los datos para finalidades incompatibles con aquellas para las que hubieran sido recogidos.

- El derecho de información del interesado se amplia en los supuestos y en el contenido de la información requerida[596].

- El derecho de oposición se incorporará como un derecho adicional a los de acceso, rectificación y cancelación.

- Se permite el tratamiento posterior de los datos y se admiten ciertas excepciones en los derechos de las personas cuando el tratamiento se realice con fines históricos, estadísticos o científicos, siempre que exista un proceso previo de disociación que no permita identificar a las personas[597].

- Se incluye la figura del encargado del tratamiento, a quien se le otorgan funciones, sobre todo en materia de seguridad, y responsabilidades derivadas del incumplimiento de sus obligaciones[598].

[594] Artículo 3 LOPD.

[595] Artículo 6.2 LOPD. No será preciso el consentimiento cuando se trate de proteger un interés vital para el interesado, o cuando se recoja de fuentes accesibles al público y su tratamiento sea necesario para la satisfacción de un interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos.
Artículo 7.6 LOPD. También se excluye el consentimiento respecto a datos especialmente protegidos cuando resulte necesario para la prevención o el diagnóstico médicos, o para la prestación de asistencia sanitaria, tratamientos médicos o gestión de servicios sanitarios en determinadas condiciones.

[596] El responsable deberá facilitar un domicilio en territorio español cuando no esté establecido en España, deberá informar al afectado en un plazo de tres meses de sus datos cuando hayan no hayan sido obtenidos por el titular, e información específica al titular cuando sus datos hayan sido obtenidos de una fuente accesible al público y se utilicen con finalidades de prospección comercial.

[597] Artículos 4.2, 4.5, 5.5, 11.1.e) y art. 21.1 LOPD.

[598] Artículos 9, 19, 37 f) y 43 LOPD.

- Se amplían las competencias de las Comunidades Autónomas[599] y se introduce un representante por comunidad autónoma con Agencia propia en el Comité Consultivo de la AEPD.

- Se mencionan por vez primera los datos personales procedentes de imágenes y sonidos[600].

- Se introduce un artículo destinado a regular el acceso a los datos por cuenta de terceros[601], cuando tal acceso sea por cuenta del responsable del fichero[602].

- Se incluye también un artículo dedicado a la figura del censo promocional, no exenta de polémica y que no ha conseguido en toda la vigencia de la ley salir adelante[603].

- Se introducen novedades respecto de la Agencia de Protección de Datos. Se aumenta el número de miembros del Consejo Consultivo[604].

- Se atribuyen nuevas funciones tanto a la Agencia como al Director[605].

- Se amplía el catálogo de infracciones así como la calificación de las mismas, y se permite evaluar una serie de parámetros para graduar los criterios y determinar la sanción.

Recursos de inconstitucionalidad.

Al igual que ocurriera con la LORTAD, la LOPD ha sido recurrida ante el Tribunal Constitucional, y es de destacar la sentencia 292/2000[606], que dictó la

[599] Artículos 40 y 41 LOPD.
[600] Artículo 3.e) LOPD.
[601] Artículo 12 LOPD.
[602] Este artículo supuso una ficción jurídica para incluirlo en una categoría distinta a la cesión de datos.
[603] Artículo 31 LOPD. El censo promocional se incluyó para dar una salida a las empresas de márketing que veían en la ley una enorme barrera a su actividad comercial. Se ha debatido en multitud de ocasiones para llevarlo a cabo pero sin resultado alguno, y es que no se ha conseguido el consenso entre las partes implicadas.
[604] Artículo 38 LOPD. Esto se hace para dar cabida a los representantes de las agencias autonómicas así como a los representantes de ficheros privados.
[605] Artículos 36 y 37 LOPD.
[606] STC 292/2000, de 30.11.2000, Pleno.
Recurso núm. 1463/2000.

inconstitucionalidad y, en consecuencia nulidad, de parte del apartado 1 del artículo 21, así como de dos incisos del apartado 1 del artículo 24 y todo el apartado 2 de dicho artículo.

Establecía la LOPD en su texto original que los datos personales recogidos o elaborados por la Administración no se podían comunicar a otras Administraciones para el ejercicio de competencias diferentes salvo cuando la cesión hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regulara su uso, o cuando la comunicación tuviera por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos[607].

La inconstitucionalidad no se refería a la cesión entre administraciones, sino que el recurso promovido por el Defensor del Pueblo tachaba de inconstitucional sólo el inciso "disposición de superior rango que regule su uso". El Tribunal entendió que no eran conformes a la Constitución ni esa excepción ni cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero, y ello porque *"la LOPD no ha fijado por sí misma, como lo impone el art. 53.1 CE, los límites al derecho a consentir la cesión de datos personales entre Administraciones Públicas para fines distintos a los que motivaron su recogida, sino que solo ha identificado la norma que puede hacerlo en su lugar"*[608].

Disponía el artículo 24 entre las excepciones a los derechos a los afectados en los ficheros de titularidad pública que "*Lo dispuesto en los apartados 1 y 2 del artículo 5 (*derecho de información*) no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte*

Recurrente: El Defensor del Pueblo.
Ponente: Julio Diego González Campos.

[607] En relación al control de datos por la Administración, ver SOUVIRÓN, J.M., *"En torno a la jurisdicción del poder informativo del Estado y el control de datos por la Administración".* Revista Vasca de Administración Pública, núm. 40, 1994, p. 121-190.

[608] STC 292/2000. Fundamentos jurídicos 15 y 19.

a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas"[609].

Para el Tribunal los motivos de limitación adolecían de tal grado de indeterminación que dejaban excesivo campo a la discrecionalidad administrativa y constituía una cesión en blanco que defrauda la reserva de ley, y además no hacía referencia a presupuestos ni condiciones de la restricción, dejando el derecho a ser informado del ciudadano del artículo 5 en la más absoluta incertidumbre, porque éste no sabrá en qué casos ocurrirá tal circunstancia, sumiendo en la ineficacia cualquier mecanismo de tutela jurisdiccional. Por lo que concluye tachando de inconstitucional los incisos referentes a la Administración: *"cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas"* y "*administrativas".*

Esa falta de certeza y previsibilidad del límite aludida por el Tribunal la hace extensible al apartado 2 del artículo 24, en que limita el derecho de acceso de los ciudadanos en interés de "lo público", declarado en pura lógica inconstitucional también este apartado.[610]

La Ley Orgánica de Protección de Datos, vigente aún en nuestros días, entró en vigor el 14 de enero de 2000. Hoy, con la redacción actual que conocemos toca a su fin. En un plazo breve sufrirá cambios importantes para adaptarse a la nueva normativa europea, si bien aún desconocemos el instrumento que se elegirá, si modificación del texto actual o una nueva ley, aunque a nuestro entender, dada la cantidad de cambios que se aproximan consideramos que el criterio adecuado sería la elaboración de un nuevo texto.

[609] En relación con el acceso de las administraciones a los datos personales, FERNANDO PABLO, M.M. *Sobre i-administración*: el Derecho administrativo de la sociedad del conocimiento (I). E-Derecho Administrativo (e-DeA) núm.9, 2003.

[610] Sobre la perspectiva de los poderes públicos: SÁNCHEZ BLANCO, A. Impulso a internet. Perspectiva de los poderes públicos. Revista del Instituto de Estudios Económicos, núm. 1-2.2001, p.389-414.

4.2.3 El Real Decreto 1720/2007.

La Disposición final primera de la LOPD[611] habilitaba al Gobierno para la aprobación del Reglamento que desarrollara la ley. Ocho años ha llevado la aprobación del mismo. La situación era de absoluta urgencia. Quienes trabajamos en la materia nos encontrábamos en esos años interpretando a diario lo que la norma parecía decir, haciéndonos eco constante de los informes jurídicos de la Agencia, los cuales acogíamos como si de jurisprudencia del Tribunal Constitucional se tratase, así como del análisis de cada resolución que publicaba la Agencia.

Además, la convivencia de reglamentos de una y otra ley hacía que el marco normativo fuera complicado. Con la LOPD, y en tanto se desarrollara el Reglamento, el legislador declaró subsistentes las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1993, de 26 de marzo, el 1332/1994, de 20 de junio, y el 994/1999, de 11 de junio, siendo los dos últimos derogados con la entrada en vigor del nuevo Real Decreto 1720/2007.

Lo que acabamos de referir tiene su constatación en la exposición de motivos, en la que el legislador recoge tres razones que se imponían en la redacción del Reglamento: la necesidad de dotar de coherencia a la regulación reglamentaria en todo lo relacionado con la transposición de la Directiva, la de desarrollar los aspectos novedosos de la Ley Orgánica 15/1999 y la de dotar de seguridad jurídica al sistema en aquellos puntos en los que la experiencia ha aconsejado un cierto de grado de precisión.

Piñar Mañas[612] relata cómo fueron los inicios del Reglamento. En los primeros meses de 2003 la Agencia inició los estudios y trabajos preparatorios para la redacción del texto. Una Comisión integrada por miembros de la Agencia y del Ministerio de Justicia redactó el primer borrador que se remitió al Ministerio a finales de 2005, borrador inicial que supuso el punto de partida sobre el que trabajar. Posteriormente

[611] Disposición final primera LOPD. *"Habilitación para el desarrollo reglamentario. El Gobierno aprobará, o modificará, las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la presente Ley"*

[612] PIÑAR MAÑAS, J.L. *Protección de datos: Origen, situación actual y retos de futuro* en El Derecho a la autodeterminación informativa. Fundación Coloquio Jurídico Europeo, Madrid, 2009, p. 138-139.

se elaboraron tres versiones más: la de 28 de noviembre de 2006, 30 de marzo de 2007 y la de 12 de julio de 2007, siendo objeto de dictamen del Consejo de Estado que dejó constancia de la gran cantidad de entidades públicas y [613]privadas así como instituciones que participaron en su elaboración vía alegaciones u observaciones.

Aportaciones:

- Entre las aportaciones más importantes del RD 1720/2007 destacamos el desarrollo de las medidas de seguridad a aplicar a los ficheros no automatizados descritas en el capítulo IV de la norma, así como la descripción de un nuevo proceso relativo al ejercicio de la potestad sancionadora (cuya instrucción no podrá ser superior a doce meses) aplicable además a determinadas infracciones cometidas al amparo de la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI)[614] así como de la ley General de Telecomunicaciones[615], que le otorgan a la AEPD competencias para ello.

- Novedad también supuso la prohibición de pedir o tratar datos de menores de catorce años sin el consentimiento de sus padres. Además, para recoger datos con información relativa a los miembros del grupo familiar o sus características se requirió que los titulares de los mismos den su consentimiento.

- Se estableció un régimen sistemático de transferencias internacionales de datos.

[613] Artículos 105 a 114 RD 1720/2007.

[614] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
BOE núm. 166, de 12.07.2002.
Artículo 43.1: "…corresponderá a la Agencia de Protección de Datos la imposición de sanciones por la comisión de las infracciones tipificadas en los artículos 38.3 c), d) e i) y 38.4 d), g) y h) de esta Ley".

[615] Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
BOE núm. 114, de 10.05.2014.
Artículo 84.3, respecto de la competencia sancionadora: "*A la Agencia Española de Protección de Datos, en el caso de que se trate de las infracciones graves del artículo 77 tipificadas en el apartado 37 y de las infracciones leves del artículo 78 tipificadas en el apartado 11 cuando se vulneren los derechos de los usuarios finales sobre protección de datos y privacidad reconocidos en el artículo 48".*

- Dejó de ser necesario el consentimiento del usuario para facilitar la asistencia sanitaria por el Sistema Nacional de Salud y facilitar la utilización de la tarjeta sanitaria individual.

- Se produjeron cambios en los niveles de determinadas categorías de datos: los datos derivados de la violencia de género pasaron del nivel básico de seguridad a un nivel alto; los ficheros de los que eran responsables los operadores de servicios de comunicaciones electrónicas disponibles al público o explotaran redes públicas de comunicaciones electrónicas sobre datos de tráfico y de localización pasaron de nivel básico a nivel medio; también de nivel básico a medio los ficheros de Entidades Gestoras y Servicios Comunes de la Seguridad Social que tuvieran relación con sus competencias y las mutuas de accidentes de trabajo y de enfermedades profesionales de la Seguridad Social. También pasaron al nivel medio de seguridad los ficheros que contuvieran datos de carácter personal sobre características o personalidad de los ciudadanos que permitieran deducir su comportamiento. Por otro lado se hizo obligatorio cifrar los datos personales incluidos en un nivel alto si se encontraban almacenados en dispositivos portátiles. Hubo un cambio de nivel, aplicándose el básico respecto de los ficheros que contuvieran datos protegidos cuando sólo se utilizaran para el pago de cuotas a las entidades de las que los titulares de los datos fueran miembros. Los datos que reflejen el grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez, cuando tengan por única finalidad cumplir una obligación legal serían catalogados de nivel básico a efectos de la aplicación de las medidas de seguridad. También se aplicaría este nivel respecto de los datos relativos a la afiliación sindical o respecto a la salud en los ficheros de nóminas.

A través del Reglamento se llevó a cabo la incorporación de antecedentes ya consolidados de las resoluciones, informes y recomendaciones de la Agencia y de las Sentencias de la Audiencia Nacional y del Tribunal Supremo, dando así respuesta a las situaciones que habían suscitado los problemas en la aplicación práctica de la ley.

El Reglamento sí dejó en vigor el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

4.2.4 Leyes sectoriales.

Muchas son las leyes que tienen relación directa con la protección de datos, algunas de las cuales ya hemos mencionado. No es objeto de este trabajo profundizar en las mismas, pero sí consideramos importante traer a colación las que entendemos de mayor relevancia:

- Ley 5/2014, de Seguridad Privada[616]
- Ley 9/2014, General de Telecomunicaciones[617];
- Ley 19/2013, de Transparencia, Acceso a la información pública y Buen gobierno[618];
- Ley 56/2007, de Medidas de Impulso de la Sociedad de la Información[619];
- Ley 37/2007, sobre reutilización de la información del sector público[620];
- Ley 25/2007, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones[621];
- Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos[622];

[616] Ley 5/2014, de 4 de abril, de Seguridad Privada.
BOE núm. 83, de 5.04.2014.
[617] Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
BOE núm. 114, de 10.05.2014.
[618] Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
BOE núm. 295, de 10.12.2013
[619] Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
BOE núm. 312, de 29.1.2007.
[620] Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
BOE núm. 276, de 17.11.2007.
[621] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
BOE núm. 251, de 19.10.2007.

- Ley Orgánica 10/2007, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN[623];
- Ley 59/2003, de Firma Electrónica[624];
- Ley 41/2002, reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica[625];
- Ley 34/2002, de Servicios de la Sociedad de la Información y del Comercio Electrónico[626];
- Ley Orgánica 4/1997 por la que se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos[627];
- Ley Orgánica 10/1995, del Código Penal[628];

[622] Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
BOE núm. 150, de 23.06.2007.
Ver LLANEZA GONZÁLEZ, P. *El valor probatorio de los archivos electrónicos.*

[623] Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.
BOE núm. 242, de 9.10.2007.

[624] Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
BOE núm. 304, de 20.12.2003

[625] Ley 41/2002, de 14 de noviembre, reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
BOE núm. 274, de 15.11.2002.

[626] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
BOE núm. 166, de 12.07.2002.
Comentarios a la ley 34/2002, CREMADES J, y GONZÁLEZ MONTES, J.L. *La nueva ley de internet*, La Ley, 2003.

[627] Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.
BOE núm. 186, de 5.08.1997.

[628] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
BOE núm. 281, de 24.11.1995.

4.3 La Agencia Española de Protección de Datos.[629]

4.3.1 Naturaleza y régimen jurídico.

La Agencia Española de Protección de Datos es la Autoridad de control nacional en materia de protección de datos en España.

Como hemos ido analizando a lo largo de este estudio, muchos han sido los instrumentos normativos y directrices que han recomendado u obligado a los Estados a la creación de estos organismos: Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales de 1980[630] y de 2013[631], 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[632], Carta de los Derechos Fundamentales de la Unión Europea de 2000[633], Protocolo Adicional del Convenio 108 del Consejo de Europa de 2001[634], Directrices para la regulación de los archivos de datos personales

[629] Inicialmente fue denominada Agencia de Protección de Datos, si bien el artículo 79 de la ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social (BOE núm. 313, de 31.12.2003) la redenominó como Agencia Española de Protección de Datos.

[630] Directrices dela OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales, de 23.09.1980.
Punto 19: *"Al implantar a nivel nacional los principios establecido en las Partes Segunda y Tercera, los Países Miembros deberían establecer procedimientos o instituciones legales, administrativos o de otro tipo para la protección de la privacidad y las libertades individuales en relación con los datos personales".*

[631] *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 2013.*
Artículo 1 d) (definiciones): *"Privacy enforcement authority means any public body, as determined by each Member country, that is responsible for enforcing laws protecting privacy, and that has powers to conduct investigations or pursue enforcement proceedings".*
Punto 19: "E*stablish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis".*

[632] Directiva 95/46/CE.
Considerando 62: *"Considerando que la creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los Estados miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales".*
Artículo 28.1*:" Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva".*

[633] Carta de los Derechos Fundamentales de la Unión Europea. DO C 364, de 18.12.2000.
Artículo 8.3: *"El respeto de estas normas quedará sujeto al control de una autoridad independiente".*

[634] Consejo de Europa, Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencia de

informatizados de 1990[635] y Resolución sobre el Derecho a la Privacidad en la Era Digital de 2013[636] de las Naciones Unidas y Estándares Internacionales sobre protección de datos y privacidad aprobados por la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad de 2009[637].

A nivel nacional, es la Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal la que otorga carta de naturaleza a la institución en su artículo 34: *"1. Se crea la Agencia de Protección de Datos. 2. La Agencia de Protección de Datos es un Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio que será aprobado por el Gobierno, así como por aquellas disposiciones que le sean aplicables en virtud del artículo 6.5 de la Ley General Presupuestaria".*

Cumpliendo el mandato de la ley, el 26 de marzo de 1993 se aprobó el Estatuto de la Agencia de Protección de Datos mediante el Real Decreto 428/1993[638] que

datos, en lo que respecta a las autoridades de control y los flujos transfronterizos de datos, CETS nº 181, 2001.
Artículo 1.1: *"Cada Parte preverá que una o más Autoridades sean responsables de asegurar la conformidad de las medidas oportunas que den cumplimiento en el Derecho interno a los principios contenidos en los Capítulos II y III del Convenio y en el presente Protocolo".*

635 Directrices para la regulación de los archivos de datos personales informatizados. Resolución 45/95 de la Asamblea General de Naciones Unidas, de 14.12.1990.
Principio 8. Supervisión y sanciones: *"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".*

636 Resolución A/C.3/68/L.45/Rev.1,de las Naciones Unidas sobre el derecho a la privacidad en la era digital, de 20.11.2013. Punto 4 d): "*To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and collection of personal data".*

637 Propuesta conjunta de Estándares internacionales de protección de la privacidad en relación con el tratamiento de datos personales. Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. Resolución de Madrid, 2009.
Artículo 23.1: *"En cada Estado existirán una o más o autoridades de supervisión que, de acuerdo con su derecho interno, serán responsables de supervisar la observancia de los principios establecidos en el presente Documento".*

638 BOE núm. 106, de 4.05.1993.

actualmente permanece en vigor, habiendo sido modificado por los Reales Decretos 156/1996[639] y 1665/2008[640].

En cuanto a la aplicación del art. 6.5 de la Ley General Presupuestaria[641], tras su derogación por la ley 6/1997 de Organización y Funcionamiento de la Administración General del Estado[642], la Agencia Española de Protección de Datos queda incluida entre las instituciones a que se refiere la disposición adicional décima de la misma, según la cual la Agencia se regirá por su normativa específica y, supletoriamente por la ley 6/1997.

Con la derogación de la LORTAD, es la LOPD la que toma el relevo legislativo en el reconocimiento de la Autoridad de control. Así, en su artículo 35 es descrita su naturaleza y su régimen jurídico[643].

---

[639] Real Decreto 156/1996, de 2 de febrero, por el que se modifica el Estatuto de la Agencia de Protección de Datos, aprobado por Real Decreto 428/1993, de 26 de marzo, para designar a la Agencia de Protección de Datos como representante español en el grupo de protección de personas previsto en la Directiva 95/46/ce, de 24 de octubre. BOE núm. 37, de 12.02.1996.

[640] 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. BOE NÚM. 267, de 5.11.008.

[641] La Ley General Presupuestaria a la que hace referencia la LORTAD es el Real Decreto Legislativo 1091/1988, de 23 de septiembre, por el que se aprueba el Texto Refundido de la Ley General , que estuvo vigente hasta el 1.01.2005.
BOE núm. 234, de 29.09.1988.

[642] Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado. BOE núm. 90, de 15.04.1997.

[643] Artículo 35 LOPD: *Naturaleza y régimen jurídico.*
"1. La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno.
2. En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En sus adquisiciones patrimoniales y contratación estará sujeta al derecho privado.
3. Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función.
4. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:
a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.
b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.

La Agencia está sujeta al derecho administrativo tanto en el ejercicio de sus competencias como en su régimen patrimonial y de contratación. Tal y como recoge el artículo 35 y sistematiza la propia Agencia en su página web[644], el régimen jurídico aplicable en el ejercicio de sus competencias es la ley 30/1992, del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común; el del régimen patrimonial es la ley 33/2003 del Patrimonio de las Administraciones Públicas (Disposición adicional quinta), y en contratación está sujeta al Real Decreto Legislativo 3/2011, por el que se aprueba el texto refundido de la ley de Contratos del Sector Público. Presupuestariamente la Agencia está sujeta a la ley 47/2003 General Presupuestaria. En materia contable ha de ajustarse al Plan General de Contabilidad Pública, estando sometida a la fiscalización por el Tribunal de Cuentas y a la Intervención General de la Administración del Estado.

4.3.2 Estructura, organización y funciones de la AEPD.

Existen dos modelos de estructura orgánica de las Autoridades de protección de datos: órgano colegiado u órgano unipersonal. En el caso de España se optó por un órgano unipersonal: el Director.

Las funciones de la Agencia Española de Protección de Datos están recogidas en el artículo 37 de la LOPD, si bien constan descritas con mayor detalle en su Estatuto[645]. También la página web de la Agencia describe algunas adicionales ejercidas dentro de cada área que han sido desarrolladas al amparo de lo dispuesto en el apartado n) del artículo 37.1, al asumir nuevas funciones atribuidas por normas legales o reglamentarias.

c) Cualesquiera otros que legalmente puedan serle atribuidos.

5. La Agencia de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado".

644 Disponible en: http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/marco-ides-idphp.php.

645 Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, BOE núm. 106, de 4.05.1993.

4.3.2.1 El Director.[646]

La Agencia ejerce sus funciones por medio de la Directora, cuyos actos se consideran actos de la Agencia. Ostenta la representación de la misma y dicta todas sus resoluciones e instrucciones, y en especial las descritas en el artículo 13 de su Estatuto.

Tal y como establece el Estatuto de la Agencia, es nombrada por el Gobierno, mediante Real Decreto a propuesta del Ministro de Justica de entre los miembros del Consejo Consultivo, y su mandato es de cuatro años[647]. Desempeña su cargo con dedicación absoluta, plena independencia y total objetividad, no estando sujeto a mandato imperativo ni recibiendo instrucciones de autoridad alguna[648].

Son **funciones** de la Directora[649]:

- Resolver motivadamente sobre la procedencia o improcedencia de las inscripciones que deban practicarse en el Registro General de Protección de Datos;
- requerir a los responsables de ficheros de titularidad privada a que subsanen deficiencias de los códigos tipo;
- resolver motivadamente, previo informe del responsable del fichero, sobre la procedencia o improcedencia de la denegación, total o parcial, del acceso a los ficheros policiales o tributarios automatizados;
- autorizar transferencias temporales o definitivas de datos que hayan sido objeto de tratamiento automatizado o recogidos a tal efecto, con destino a países cuya legislación no ofrezca un nivel de protección equiparable al de la LOPD;

[646] Actualmente Directora. María del Mar España Martí ha sido nombrada Directora de la Agencia Española de Protección de Datos por el Real Decreto 715/2015, de 24 de julio. BOE núm. 177, de 25.07.2015.
[647] Artículo 14 Estatuto AEPD.
[648] Artículo 16 Estatuto AEPD.
[649] Artículo 12 Estatuto AEPD.

- convocar regularmente a los órganos competentes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación;
- recabar de las distintas Administraciones Públicas la información necesaria para el cumplimiento de sus funciones;
- solicitar de los órganos de las Comunidades Autónomas con competencias en protección de datos la información necesaria para el cumplimiento de sus funciones, así como facilitar a aquéllos la información que le soliciten a idénticos efectos;
- adoptar las medidas cautelares y provisionales que requiera el ejercicio de la potestad sancionadora de la Agencia con relación a los responsables de los ficheros privados;
- iniciar, impulsar la instrucción y resolver los expedientes sancionadores referentes a los responsables de los ficheros privados;
- instar la incoación de expedientes disciplinarios en los casos de infracciones cometidas por órganos responsables de ficheros de las Administraciones Públicas;
- autorizar la entrada en los locales en los que se hallen los ficheros, con el fin de proceder a las inspecciones pertinentes, sin perjuicio de la aplicación de las reglas que garantizan la inviolabilidad del domicilio;
- la representación en el ámbito internacional;
- funciones de gestión (adjudicar contratos, aprobar gastos y ordenar pagos, programar la gestión de la Agencia, elaborar el anteproyecto de la Agencia, aprobar la Memoria anual, ejercer el control económico-financiero, proponer la relación de puestos de trabajo y ordenar la convocatoria de reuniones del Consejo Consultivo).

Existe una **Unidad de Apoyo** a la Directora formada por el Gabinete Jurídico, el Adjunto al Director, el Área Internacional y el Gabinete de Comunicación y prensa.

A. Gabinete Jurídico.

Está integrado por miembros de la Abogacía del Estado.

Sus funciones son:

- Coordinación de la asistencia jurídica a la Agencia Española de Protección de Datos.
- Emisión de dictámenes jurídicos a los sectores público y privado en relación con la interpretación y aplicación de la normativa de protección de datos.
- Emisión de propuestas de dictámenes preceptivos a los Proyectos normativos que afectan a protección de datos, así como a los exigidos preceptivamente por la normativa sectorial (telecomunicaciones, prevención de blanqueo de capitales, legislación sobre juego, etc.).
- Vocalía de la Comisión de Transparencia y Buen Gobierno en representación de la Agencia.

B. Adjunto al Director.

El Adjunto al Director da apoyo a las funciones de Dirección de la Agencia, colaborando en las relaciones institucionales que desarrolla la Agencia y con las diferentes unidades que conforman la institución.

C. Gabinete de Prensa y Comunicación.

Tiene las siguientes funciones:

- Apoya y asesora a la Dirección de la Agencia en materia de comunicación.
- Impulsa la difusión de la actividad de la Agencia en medios con objeto de fomentar una cultura de protección de datos entre ciudadanos y organizaciones.

- Promueve la comunicación interna y externa de la AEPD.
- Asesora en la promoción de la imagen pública de la Agencia.

D. Área internacional.

Desarrolla las siguientes funciones:

- Asesoramiento y apoyo a la Dirección de la Agencia en materia de relaciones internacionales.
- Ejecución de la política de relaciones internacionales de la Agencia, de acuerdo con los criterios y directrices establecidos por la Dirección.
- Representación internacional de la Agencia.
- Información y apoyo a las unidades de la Agencia.
- Coordinación de la actividad internacional de las unidades de la Agencia.

Esta área tiene una gran importancia dentro de la Agencia, cuyo trabajo y proyección es cada vez mayor, habiéndose convertido en referente internacional.

Participa como miembro en las siguientes organizaciones y grupos de trabajo:

· Grupo de Trabajo del Artículo 29.

· Comité Consultivo del Convenio 108 del Consejo de Europa.

· Conferencia de Primavera de las Autoridades europeas de protección de datos.

· Grupo de Telecomunicaciones de Berlín.

· Encuentro Ibérico de Protección de Datos (junto a Portugal).

· Red Iberoamericana de Protección de Datos.

· Conferencia Internacional de Autoridades de Protección de Datos.

También participa en el Taller de Gestión de Reclamaciones (*Case Handling Workshop*), que es un grupo de trabajo que se creó en el seno de la Conferencia de Primavera.

A nivel de cooperación policial y judicial en la Unión Europea, participa en la Europol (Oficina Europea de Policía), y en Eurojust. También lo hace en el Sistema de Información *Schengen* de segunda generación (SIS II). La Agencia Española de Protección de Datos ejerce las funciones de Autoridad Nacional de Control en Europol[650], y ejerce el control de los datos de carácter personal introducidos en la parte nacional española de la base de datos del Sistema de Información *Schengen* (SIS)[651]. En relación con el control de fronteras y aduanas, interviene en el Sistema de Información Aduanero (SIA), en el Sistema de Información de Visados (SIV) y en Eurodac.

4.3.2.2 El Consejo Consultivo.

Es un órgano colegiado de carácter consultivo, cuyas funciones son asesorar al Director emitiendo informes en las cuestiones que éste le someta y formulando propuestas en materia de protección de datos cuando así lo considere.

Sus diez miembros son representantes de los distintos sectores de la sociedad con implicación en el tratamiento de datos personales. Son nombrados por el Ministro de Justicia, pero propuestos por distintas instituciones a las que representan[652]: el

[650] Decisión del Consejo de 6 de abril de 2009 (2009/371/JAI). DOUE de 15 de mayo de 2009. L 121. Artículo 33, respecto de la obligatoriedad de tener una autoridad de control nacional: *"cuya tarea consistirá en vigilar, de manera independiente y con arreglo a la legislación nacional, la licitud de la introducción, la consulta de datos y todo tipo de transmisión de datos personales a Europol por parte del Estado miembro de que se trate, y en verificar que no se vulneran los derechos de las personas a las que se refieren los datos".*

[651] Convenio de aplicación del Acuerdo Schengen, 14 de junio de 1985 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.
DO L 239, de 22.09.2000
Artículo 114: La Autoridad Nacional se encarga de *"ejercer un control independiente sobre el fichero de la parte nacional del Sistema de Información de Schengen y de comprobar que el tratamiento y la utilización de los datos introducidos en el Sistema de Integración de Schengen no atentan contra los derechos de la persona de que se trate".*

[652] Artículo 19 Estatuto AEPD.

Congreso de los Diputados, el Senado, la Administración General del Estado (a través del Ministro de Justicia), las Comunidades Autónomas, la Administración local (a través de la Federación Española de Municipios y Provincias), la Real Academia de Historia, el Consejo de Universidades, el Consejo de Consumidores y Usuarios y el Consejo Superior de Cámaras de Comercio, Industria y Navegación. La duración de sus cargos es de cuatro años.

Al Consejo le es de aplicación la Ley 30/1992, de 26 de noviembre, del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común[653], que rige para los órganos administrativos colegiados.

4.3.2.3 El Registro General de Protección de Datos.

El Registro General de Protección de Datos está organizativamente constituido como una Subdirección General.

Son funciones del Registro las siguientes:

- Velar por la publicidad de los tratamientos de datos y por el ejercicio del derecho de consulta.
- Inscribir los ficheros de los que sean titulares las Administraciones públicas y los de titularidad privada, así como sus modificaciones, supresión o cancelación.
- Inscripción de las autorizaciones de transferencias internacionales de datos.
- Inscripción de los códigos tipo.
- Inscripción de la autorización de conservación de datos para fines históricos, estadísticos o científicos.

Esta área de la Agencia será una de las que se verán más afectadas cuando entre en vigor el nuevo Reglamento General de Protección de Datos europeo.

[653] Ley 30/1992, de 26 de noviembre, del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Capítulo II del Título II. BOE núm. 285, de 27.11.1992.

Según datos facilitados por la propia Agencia en su web[654], el número de ficheros inscritos a 30 de septiembre de 2015 es de 4.029.816, de los cuales 156.080 son de titularidad pública, y 3.873.736 de titularidad privada. Sin embargo, con el nuevo Reglamento, a priori, parece que desaparecerá la obligatoriedad de la inscripción de los ficheros, ya que se pretende reducir las cargas administrativas asociadas al cumplimiento de la normativa. Desconocemos en qué términos quedará finalmente esta situación, pero lo cierto es que no aparece dicha obligación en los textos del nuevo Reglamento europeo.

El Registro seguirá teniendo algunas de sus competencias actuales, pero el órgano deberá renovarse y adaptarse a los nuevos tiempos. Entendemos que continuará siendo el encargado de tutelar las autorizaciones de transferencias internacionales, las denuncias y las consultas, pero además será probablemente el competente para tutelar los procedimientos realizados en tratamientos que presenten riesgos y hayan de ser previamente notificados a la Autoridad de control, o quizás también aquellos en los que la Agencia tenga conocimiento en el ejercicio de un procedimiento sancionador, y probablemente sea el organismo encargado de tutelar las notificaciones de violaciones del derecho a la protección de datos y todos los procedimientos relacionados con certificación. En definitiva, un nuevo tiempo llega a la Agencia Española de Protección de Datos.

4.3.2.4 La Inspección de Datos.

Organizativamente, al igual que el Registro General de Protección de Datos, es una Subdirección General. Es el órgano que ejerce la función inspectora de la Agencia[655].

La Inspección de Datos aglutina tanto las funciones propias de la inspección como las de la instrucción de los procedimientos.

A. Funciones de inspección:

[654] Disponible en: http://www.agpd.es/portalwebAGPD/ficheros_inscritos/estadisticas/common/pdfs/2015/est201509.Pdf.
[655] Artículo 40 LOPD.

- En el ejercicio de la potestad sancionadora, efectúa las inspecciones de oficio o a instancia de parte previa denuncia en los locales en los que se hallen los ficheros y los equipos informáticos correspondientes, tanto para ficheros de titularidad pública o privada, previa autorización expedida por la Directora de la Agencia. Para ello podrán:
    - Examinar los soportes de información y los equipos físicos que contengan datos personales.
    - Examinar los programas informáticos y los sistemas de transmisión y acceso a los datos.
    - Realizar auditorías de los sistemas informáticos para determinar su adecuación con la normativa.
    - Requerir la exhibición y/o el envío de cualesquiera documentos e información pertinentes.
- Hace inspecciones de carácter preventivo realizando auditorías para posteriormente elaborar propuestas de mejora a los distintos sectores afectados.
- Lleva a cabo procedimientos de tutela de los derechos ARCO[656], según lo previsto en el capítulo II del Título IX del RD 1720/2007.
- Analiza las notificaciones de quiebras de seguridad a las que se refiere el artículo 41 de la LGT[657], pudiendo examinar las medidas adoptadas por los operadores con objeto de proponer las oportunas recomendaciones sobre las mejores prácticas con respecto al nivel de seguridad que debería conseguirse con tales medidas.

[656] Los derechos ARCO son los derechos de acceso, rectificación, cancelación y oposición de los interesados.

[657] Ley General de Telecomunicaciones.
Que viene a trasponer la importante 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.

Los responsables del fichero que se pretendan inspeccionar están obligados a permitir el acceso a los locales en los que se hallen los ficheros y los equipos informáticos. Sin embargo, cuando los locales tengan la consideración legal de domicilio, la labor inspectora deberá ajustarse además a las reglas que garantizan su inviolabilidad.

B. Funciones de instrucción.

- Tramitar los procedimientos sancionadores y de declaración de infracción, tanto de entes privados como públicos[658] previamente incoados por los inspectores.

- Llevar a cabo los procedimientos de exención del deber de información al interesado[659].

El ejercicio de la potestad sancionadora de la Agencia Española de Protección de Datos le es atribuido por la Ley Orgánica de Protección de Datos en todo lo que a protección de datos se refiere; por la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico en cuanto a las infracciones por incumplimiento de la normativa de *spam* y *cookies*; y por la Ley General de Telecomunicaciones[660] en los procedimientos instados sobre llamadas automáticas sin intervención humana o mensajes de fax, con fines de comunicación comercial.

El proceso de inspección de la AEPD es un proceso justo. Está descrito en el Real Decreto 1720/2007 en los procedimientos relativos al ejercicio de la potestad sancionadora. En la fase de inspección el inspector recopila información y evidencias, y en la de instrucción es el instructor quien, a la vista del expediente presentado, califica y lleva a cabo el procedimiento, para finalmente proponer o no sanción.

[658] Secciones 3ª y 4ª del capítulo III del Título IX del RD 1720/2007.
[659] Capítulo VII del Título IX RD 1720/2007.
[660] Sobre la normativa en telecomunicaciones:
CREMADES, J. y RODRÍGUEZ ARANA, J. (Dirs), *Comentarios a la Ley General de Telecomunicaciones (aprobada por Ley 32/2003, de 3 de noviembre)*, La Ley, Madrid, 2004.

Un poder de intervención claro y no discutido es base fundamental para calificar de independiente a una autoridad de control. Este hecho marca la diferencia entre las autoridades de control, pues no se ejerce de igual modo el poder si existe habilitación para inspeccionar cualesquiera tipo de entidades públicas o privadas, pudiendo acceder a sus instalaciones y solicitar cuanta información se precise que si no se tiene. La Agencia española detenta dicho poder de forma clara, mientras que otras como la Autoridad de control del Reino Unido, *the Information Commissioner's Office* (ICO), no puede por ejemplo auditar ni inspeccionar a las empresas privadas, y sí puede hacerlo en la administración pública. Esta situación va progresivamente cambiando en Europa siguiendo las tesis de la Agencia española.

4.3.2.5 La Secretaría General.

La Secretaría General tiene funciones de apoyo a las distintas unidades de la Agencia así como la llevanza de la Secretaría del Comité Consultivo.

Tiene varias áreas: Informática, Atención al Ciudadano, Administración General y Documentación y Estudios.

4.3.3 La independencia.

Tal y como analizamos en el capítulo II al profundizar sobre la independencia de las Autoridades de control, es ésta una característica básica y no discutible en los organismos de control en materia de protección de datos.

Según Puente Escobar[661], en el derecho comparado europeo la independencia se manifiesta en formas distintas: hay Autoridades de control que se configuran como órgano colegiado, en las que se integran representantes de los distintos poderes del estado, como Portugal (*Comissão Nacional de Protecção de Dados*), Francia

[661] PUENTE ESCOBAR, A. *La Agencia Española de Protección de Datos como garante del derecho fundamental a la protección de datos de carácter personal*. Azpilcueta. Cuadernos de Derecho, 20. San Sebastián 2008, p. 26.
Agustín Puente es actualmente Jefe del Gabinete jurídico de la AEPD.

(*Commission Nationale de l'Informatique et des Libertés* –CNIL-) o Italia (*Garante per la protezione dei dati personali*); otras son nombradas directamente por el Parlamento y no por el Gobierno, como Hungría *(Data Protection Commissioner of Hungary*); en países como República Checa (*The Office for Personal Data Protection)* no sólo el director es nombrado por el Parlamento, sino parte del propio personal del órgano; en otras ocasiones aunque los órganos rectores sean nombrados por el Gobierno la propia naturaleza de la institución así lo indica, como es el caso de Países Bajos *(College bescherming persoonsgegevens Dutch Data Protection Authority)* o Austria (*Österreichische Datenschutzbehörde).*

En el caso de España, la cualidad de la independencia viene recogida en el artículo 35.1 de la LOPD: "…*actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones*…". Esta afirmación es desarrollada en el artículo 1.2 del Estatuto de la Agencia: *"La Agencia de Protección de Datos actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones y se relaciona con el Gobierno a través del Ministerio de Justicia".*

Siguiendo a Puente Escobar[662], la AEPD no está incluida en la estructura orgánica de ningún órgano de la Administración del Estado, cosa que sí ocurre en otros organismos reguladores tales como la Comisión Nacional del Mercado de Valores, la Comisión Nacional de las Telecomunicaciones, la Comisión Nacional de la Energía o el propio Tribunal de Defensa de la Competencia. Según el autor, la independencia de la Agencia Española de Protección de Datos es plena pues no existe relación jerárquica alguna, *"la Ley únicamente atribuye al Ministerio de Justicia la función de ser el punto de comunicación de la Agencia con la Administración General del Estado, pero en ningún caso somete a aquella al ámbito de dicho departamento"*, llegando a comparar a la Agencia con el Banco de España.

Tellez Aguilera[663] sistematiza las características de la independencia de la Agencia Española de Protección de Datos en varios aspectos: el hecho de que el director sólo pueda ser removido de su cargo por causas legalmente tasadas (art. 36.3 LOPD); que

[662] Ídem. P. 26-27.
[663] TÉLLEZ AGUILERA, A. *Nuevas tecnologías, intimidad y protección de datos*. Madrid, Edisofer, 2001; p. 211.

en el cumplimiento de sus funciones no esté sujeto a las instrucciones de ninguna otra autoridad (art. 36.2 LOPD); que la Agencia cuente con una autonomía patrimonial y presupuestaria (arts. 35.4 y 35.5 LOPD); que la Memoria Anual se remita al Ministerio de Justicia no como destino final, sino para que éste la haga llegar a las Cortes Generales (art. 8 del Estatuto de la Agencia); y que sólo se relacione con el Gobierno a través de este Ministerio (art. 1.2 del Estatuto de la Agencia).

A pesar de coincidir en todas las cualidades descritas que nos llevan a sentenciar que la independencia de la Agencia Española de Protección de Datos es real, desde nuestro punto de vista el hecho de que el nombramiento de su Director sea realizado por el Gobierno a propuesta del Ministro de Justicia de entre los miembros del Comité Consultivo en el que el propio Gobierno ha designado un miembro permite cuestionar la tan invocada independencia. Creemos que para paliar en cierta medida este hecho se ha establecido que el nombramiento vaya precedido de un dictamen del Congreso en el que se determine su idoneidad o no para el cargo, tal y como establece la disposición adicional tercera de la ley 3/2015 reguladora del ejercicio del alto cargo de la Administración General del Estado, si bien dicho dictamen no parece vinculante a la vista del texto normativo[664]. Consideramos que sería más idóneo a fin de constatar la independencia del ente que su nombramiento fuera realizado por el Parlamento con mayoría cualificada y no por el Gobierno[665].

[664] Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado.
BOE núm. 77, de 31.03.2015.
"Disposición adicional tercera. Comparecencia ante el Congreso de los Diputados.
1.- Con carácter previo a su nombramiento, el Gobierno pondrá en conocimiento del Congreso de los Diputados, a fin de que pueda disponer su comparecencia ante la Comisión correspondiente de la Cámara, el nombre de los candidatos para los siguientes cargos: … e) Director de la Agencia Española de Protección de Datos".
2.- La Comisión parlamentaria del Congreso de los Diputados examinará, en su caso, a los candidatos propuestos. Sus miembros formularán las preguntas o solicitarán las aclaraciones que crean convenientes. La Comisión parlamentaria emitirá un dictamen en el que se pronunciará sobre si se aprecia su idoneidad o la existencia de conflicto de intereses".

[665] Muchos autores coinciden con esta crítica. Así, HERRÁN ORTIZ, I. *La violación de la intimidad en la protección de datos personales*, 1999, p. 344 y 346; DÁVARA RODRÍGUEZ, M. A. *La Ley española de protección de datos (LORTAD): ¿una limitación del uso de la informática para garantizar la intimidad?,* AJA, núm. 76/77, 1992, p.3. En sentido contrario, Heredero Higueras opina que "el hecho de que la designación del Director se haga por el Gobierno es irrelevante desde el punto de vista de su independencia, pues la designación parlamentaria, en sí misma, también

4.3.4 El nuevo marco regulador de las Autoridades de control en el Reglamento General de Protección de Datos.

El nuevo Reglamento General de Protección de datos tiene como objetivo básico la armonización normativa en materia de protección de datos en los países de la Unión. Pero le acompañan dos objetivos más, hacer frente a la situación tecnológica actual dejando la puerta abierta para todos los cambios que previsiblemente surjan a medio plazo, y fortalecer los derechos de los ciudadanos.

El papel de las Autoridades de Control es fundamental. Serán las encargadas de velar por el cumplimiento de la norma y tener un papel muy proactivo en todas las fases del tratamiento de datos.

La Agencia Española de Protección de Datos ha sido pionera en muchos aspectos, y ha conseguido que el nivel de protección de datos en las grandes empresas en España sea muy superior a las del resto de la Unión Europea.

A pesar de ello, tras veinte años desde la Directiva y dieciséis desde la entrada en vigor de nuestra LOPD, las necesidades de supervisión y control han evolucionado. La AEPD continuará llevando a cabo la mayoría de las funciones que hasta ahora venía desempeñando, pero hay que mirar a Europa, y las funciones se van a ver incrementadas en gran medida.

Tras un análisis de las propuestas de Reglamento, y teniendo en cuenta que se barajan tres textos, aun no sabiendo cómo quedarán determinadas muchas de las nuevas funciones, a continuación describimos algunas de ellas que entendemos

puede acarrear un riesgo de politización, en la medida en que la elección de su titular o titulares pueda estar mediatizada por la correlación de las fuerzas políticas". HEREDERO HIGUERAS, M. *La Agencia de Protección de Datos*, Informática y Derecho núm. 6 y 7, UNED, Mérida, 1994, p. 326.

novedosas para la Agencia Española de Protección de Datos[666], obviando en este listado las que a nuestro juicio ya desempeña la Agencia:

- Adoptar cláusulas contractuales estándar. Art. 26.2.quarter.
- Recepcionar los registros de categorías de los responsables y encargados del tratamiento. Art. 28.3.
- Recepcionar notificaciones en los casos de violación de datos personales que probablemente vayan a dar lugar a un alto riesgo para los derechos y libertades de los interesados[667]. Es el conocido como *data breach*. Art. 31.1.
- Elaborar y publicar una lista de los tipos de operaciones de tratamiento que estarán supeditados a una evaluación de impacto, la cual deberá ser comunicada al Consejo Europeo de Protección de Datos. Art. 33.2.bis.
- Podrá publicar una lista de tratamientos que no requieren evaluación de impacto y ser comunicada al Consejo Europeo de Protección de Datos. Art. 33.2.ter.
- Aplicar el mecanismo de coherencia del art. 57 a esas listas si incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión. Art. 33.2.quarter.
- Recibir consultas de los responsables del tratamiento respecto de los tratamientos de riesgo cuando la evaluación de impacto indique que, a falta de medidas por parte del responsable para mitigarlo, éste entrañe un nivel de riesgo elevado. Art. 34.2.

[666] Los artículos a los que se hace referencia pertenecen al texto presentado por el Consejo de la Unión Europea el 11 de junio de 2015.

[667] Tales como problemas de discriminación, usurpación de identidad o fraude, pérdidas económicas, cambio no autorizado de la seudonimización, menoscabo de la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional o cualquier otro perjuicio económico o social significativo. Art. 31.1.

- Asesorar al responsable del tratamiento cuando la Autoridad considere que éste no es conforme a lo previsto en el Reglamento y no se haya identificado o atenuado el riesgo, facilitándole la información descrita en el apartado 6. Art. 34.3.

- Recibir consultas de los responsables de los tratamientos cuando dichos tratamientos sean en el ejercicio de una labor de interés público. Art. 34.7 bis.

- Recibir los datos de contacto de todos los delegados de protección de datos. Art. 35.9.

- Promover la elaboración de códigos de conducta; emitir dictámenes sobre los proyectos de códigos de conducta o sus modificaciones; y proceder al registro y publicación de los mismos. Art. 38.1,2 y 2.bis. Si el código de conducta aplica tratamientos en varios Estados miembros, la autoridad de control competente deberá someterlo al Consejo Europeo de Protección de Datos para su aprobación. Art. 38.2.ter.

- Fomentar la creación de mecanismos de certificación y de sellos y marcas, y aprobar los criterios de certificación. Art. 39.2 bis.

- Llevar a cabo, si procede, una revisión periódica de las certificaciones expedidas. Art. 39.4.

- Elaborar y publicar los criterios para la acreditación de un organismo de supervisión de los códigos de conducta, art. 38 bis; y para los organismos de certificación, art. 39 bis.

- Efectuar la acreditación de un organismo de supervisión de los códigos de conducta, art. 38 bis; y de un organismo de certificación, art. 39 bis.

- Aprobar normas corporativas vinculantes de conformidad con el mecanismo de coherencia establecido en el artículo 57. Art. 43.

- Tomar medidas apropiadas para crear mecanismos de cooperación internacional con terceros países y organizaciones internacionales. Art. 45.1.

- Acordar los procedimientos y recursos necesarios para llevar a cabo el mecanismo de ventanilla única *(one-stop-shop)*[668]. Art. 51 bis.
- Cooperar y compartir información con otras autoridades de control. Art. 52.1.c).
- Seguimiento de las novedades de interés. Art. 52.1.e).
- Contribuir a las actividades del Consejo Europeo de Protección de Datos. Art. 52.1.j).
- Arbitrar los mecanismos necesarios para que se lleve a cabo el mecanismo de cooperación entre la autoridad de control principal y las demás autoridades de control afectadas, 54 bis; así como para las operaciones conjuntas; Art. 56.
- Arbitrar los procedimientos y recursos necesarios para aplicar el mecanismo de coherencia del artículo 57. Art. 57.

Como decíamos, además de las funciones arriba descritas seguirán llevándose a cabo la mayoría de las que ahora desempeñan, con la gran excepción (ya apuntada) de la inscripción de los ficheros que debemos entender, a la vista de los textos, que desaparece.

Por lo tanto, la situación de cambio a la que la Agencia Española de Protección de Datos se enfrenta requerirá de medios y esfuerzos notables para realizar todas las funciones y competencias que el nuevo Reglamento General de Protección de Datos le encomienda. Se hace necesario a todas luces una reestructuración del organismo para adaptarse a los nuevos tiempos, donde el personal deberá tener, además de las aptitudes hasta ahora ampliamente demostradas, conocimientos en idiomas y en derecho comparado, pues gran parte de las nuevas competencias se desarrollarán en el encuentro o desencuentro entre los distintos países de la Unión Europea.

[668] El principio de "*one-stop-shop*" consiste en adjudicar a una sola autoridad la competencia para supervisar las actividades del responsable o encargado del tratamiento en toda la Unión cuando el tratamiento se realiza en varios Estados miembros. La propuesta establece que la competencia recaiga sobre la autoridad supervisora del Estado miembro en el que el responsable tenga su establecimiento principal.

4.3.5 La Agencia Española de Protección de Datos y el Consejo de la Transparencia.

El derecho a la protección de datos no es un derecho absoluto, sino que ha de relacionarse con su función en la sociedad[669]. Esa afirmación hoy ya no es discutida y ha sido refrendada tanto por la jurisprudencia europea[670] como por la española. Ningún derecho es absoluto, pero la ponderación entre ellos no siempre es fácil. El equilibrio entre el derecho de acceso a la información y el derecho a la protección de datos tiene unos límites muy finos.

El derecho a la protección de datos está reconocido como derecho fundamental en el artículo 8 de la Carta de los Derechos Humanos y en el artículo 18.4 de la Constitución Española; y el derecho de acceso a la información pública es un derecho fundamental del artículo 42 de la Carta de los Derechos Fundamentales[671], y en nuestro texto constitucional si bien está recogido en el artículo 105 b) de la misma, no lo hace como derecho fundamental.

[669] Tal y como dice la Comisión Europea en la Exposición de Motivos de la Propuesta de Reglamento General de Protección de Datos *"En consonancia con el artículo 52, apartado 1, de la Carta, pueden introducirse limitaciones al ejercicio del derecho a la protección de datos, siempre que tales limitaciones estén establecidas por ley, respeten el contenido esencial de dichos derechos y libertades y, respetando el principio de proporcionalidad, 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"*.

[670] Sentencia del Derecho al Olvido.
Sentencia TJUE (Gran Sala), de 13.05.2014. Asunto C-131/12. Google vs AEPD y Mario Costeja.
Ver 193.
Sentencia TJCE de 20.05.2003, As. C-465/00, C-138/01 y C-139/01, Caso *Rechnungshof contra Österreichischer Rundfunk.*
Ver 169.
Sentencia TJUE (Gran Sala), de 29.06.2010. Asunto C-28/08 P), Caso *Comisión contra Bavarian Lager.*
Ver 227.
Sentencia TJUE de 9.11.2010. Asuntos acumulados C-92/09 y C-93/09. Caso *Volker und Markus Schecke y Eifert.*

[671] Carta de los Derechos fundamentales. DO C 364, de 18.1.2000.
Artículo 42: *"Todo ciudadano de la Unión o toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro tiene derecho a acceder a los documentos del Parlamento Europeo, del Consejo y de la Comisión".*

En el año 2013 se dictó en España la Ley 19/2013[672], de Transparencia, Acceso a la Información Pública y Buen Gobierno, la cual prevé en su disposición adicional quinta que "*El Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos adoptarán conjuntamente los criterios de aplicación, en su ámbito de actuación, de las reglas contenidas en el artículo 15 de esta Ley*".[673]

Establece el artículo 15 de esta ley que cuando el acceso se pretenda sobre datos especialmente protegidos se deberá obtener el consentimiento expreso y escrito del afectado en unos casos y escrito en otros. Pero *"cuando la información solicitada no contenga datos especialmente protegidos el órgano al que se dirija la solicitud concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular su derecho fundamental a la protección de datos de carácter personal".*

El gran quiz de la cuestión es cómo realizar esa ponderación de los derechos. Para ello, la ley 19/2013 establece una serie de criterios que el órgano deberá considerar:

- El menor perjuicio a los afectados derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español respecto de la consulta de los documentos.

- La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos.

- El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquéllos.

[672] Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. BOE núm. 295, de 10.12.2013.

[673] Sobre derecho a información y transparencia, CRUCES BLANCO, E. *Los portales de la transparencia: Derecho a la información, transparencia y toma de decisiones, ¿leyes transparentes o translúcidas?* Boletín ACAL, núm. 95, 2015, p. 5-7.

- La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad.

La Ley de Transparencia establece también que la normativa de protección de datos será de aplicación a los tratamientos posteriores de los datos obtenidos por el derecho de acceso a los mismos, y que estos criterios no serán de aplicación para el caso de previa disociación de los datos personales en la información obtenida.

Pues bien, el trabajo en equipo de ambos organismos, Agencia Española de Protección de Datos y Consejo de Transparencia ya ha comenzado su periplo. Su primer dictamen conjunto[674] fue publicado en marzo de 2015, y tiene causa en la consulta realizada por la Directora de la Oficina para la Ejecución de la Reforma de la Administración (OPERA) del Ministerio de la Presidencia, a fin de adoptar un criterio uniforme sobre la posibilidad de admitir y dar acceso a la información sobre la retribución de determinados cargos públicos, las Relaciones de Puestos de Trabajo de los distintos órganos administrativos así como la identidad de la persona que desempeña un determinado puesto de trabajo y la productividad percibida por cada empleado público de manera individualizada. Es de resaltar en dicho informe la diferencia destacada sobre el acceso a la información y la publicidad activa.

El Consejo de Transparencia y Buen Gobierno está regulado en su Estatuto[675], en cuya estructura figura la Comisión de Transparencia y Buen Gobierno, un organismo que, entre otras funciones, es el encargado de asesorar e informar en la materia. Un representante de la Agencia Española de Protección de Datos[676] forma parte de la composición de dicho organismo, cargo que actualmente desempeña el Jefe del Gabinete Jurídico de la AEPD.

[674] Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/criterios_art_15/index-ides-idphp.php.

[675] Real Decreto 919/2014, de 31 de octubre, por el que se aprueba el Estatuto del Consejo de Transparencia y Buen Gobierno.
BOE núm. 268, de 5.11.2014.

4.4 Las autoridades de control autonómicas.

4.4.1 Referentes normativos.

El Protocolo Adicional al Convenio 108 del Consejo de Europa[677] así como la Directiva 95/46/CE[678] recogían la posibilidad de que los Estados parte tuviesen más de una Autoridad de control en su territorio. El Considerando 92 del nuevo Reglamento General de Protección de Datos recoge la creación por los Estados miembros de más de una Autoridad de control a fin de reflejar su estructura organizativa o administrativa.[679]

Preámbulo de las competencias otorgadas en España a las Comunidades Autónomas en materia de supervisión y control de la protección de datos de carácter personal lo supuso, tal y como recogíamos en el apartado dedicado a la LORTAD[680], la proposición de ley presentada por el entonces Grupo Parlamentario de Coalición Popular en 1987 sobre la protección al honor y a la intimidad de las personas frente a la utilización de las bases de datos[681]. Llamaba nuestra atención por cuanto dedicaba un capítulo a la Inspección de protección de datos, recogiendo en su artículo décimo que *"las Comunidades Autónomas podrán crear, en el ámbito de sus competencias y territorio las correspondientes Inspecciones de Protección de Datos",* figura equivalente a las actuales Autoridades de control.

El artículo 40 de la Ley Orgánica 5/1992 (LORTAD) establecía la posibilidad de que órganos de control autonómicos ejercieran determinadas funciones de las

[677] Artículo 1 Protocolo Adicional del Convenio 108: *"Cada Parte preverá que una o más Autoridades sean responsables de asegurar la conformidad de las medidas oportunas que den cumplimiento en el Derecho interno a los principios contenidos en los Capítulos II y III del Convenio y en el presente Protocolo".*

[678] Artículo 28.1 Directiva 95/46/CE: *"Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva".*

[679] Considerando 92 Reglamento General de Protección de Datos, versión Consejo: *"La creación en los Estados miembros de autoridades de control que ejerzan sus funciones con plena independencia constituye un elemento esencial de la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal. Los Estados miembros pueden crear más de una autoridad de control con objeto de reflejar su estructura constitucional, organizativa y administrativa."*

[680] Apartado 4.2.1.

[681] BOCG de 27.04.1987, serie B, núm. 68-I.

ejercidas por la Agencia española cuando afectaran a ficheros automatizados de datos de carácter personal creados o gestionados por las Comunidades Autónomas, a los que se garantizaría plena independencia y objetividad en el ejercicio de su cometido.

Al amparo de esa disposición, la Comunidad de Madrid creó la primera Agencia de Protección de Datos autonómica en virtud de la ley 13/1995, de regulación del uso de la informática en el tratamiento de datos personales[682], comenzando su andadura en julio de 1997. Tras la entrada en vigor de la LOPD se aprobó la ley 8/2001 de Protección de Datos de Carácter Personal en la Comunidad de Madrid, que adaptaba su contenido a la nueva previsión legislativa[683]. Mediante Decreto 67/2003 se aprobó el Reglamento de desarrollo de las funciones de la agencia respecto de la tutela del derecho[684]. No obstante, por razones de racionalización del gasto público, la Agencia de Protección de Datos de la Comunidad de Madrid fue suprimida con fecha 1 de enero de 2013[685].

Serán los artículos 41 y 42 de la Ley Orgánica 15/1999, LOPD, los que recojan las referencias y competencias en materia de protección de datos de las comunidades autónomas. El artículo 41 amplía el ámbito de actuación de las Autoridades de control autonómicas al extenderla sobre los ficheros de datos de carácter personal

[682] Ley 13/1995, de 21 de abril, de regulación del uso de la informática en el tratamiento de datos personales por la Comunidad de Madrid.
BOCM núm. 105, de 4.05.1995 y BOE núm. 170, de 18.07.1995.
(Modificada por la ley 13/1997, de 16 de junio de modificación de la ley 13/95, de 21 de abril, de regulación del uso de la informática en el tratamiento de datos personales por la Comunidad de Madrid. BOCM núm. 148, de 24.06.1997; y por la Ley 6/1999, de 30 de marzo, de modificación del párrafo cuarto del artículo 27.6 de la Ley 13/1995, de 21 de abril, de regulación del uso de la informática en la Comunidad de Madrid. BOE núm. 127, de 28.05.1999).
Art. 7: "*1. Se crea la Agencia de Protección de Datos de la Comunidad de Madrid como Ente de Derecho Público de los previstos en el artículo 6 de la Ley 9/1990, de 8 de noviembre, reguladora de la Hacienda de la Comunidad de Madrid, con personalidad jurídica propia y plena capacidad de obrar".*

[683] Suprimía todas las referencias contenidas en la Ley 13/1995 relacionadas con la recogida de datos de carácter personal, los derechos de los ciudadanos y el principio del consentimiento, el ejercicio de los derechos de acceso, cancelación y rectificación o la cesión de datos entre otros, ya que eran aspectos que quedaban bien delimitados en la nueva ley.

[684] Decreto 67/2003, de 22 de mayo. BOCAM de 2.06.2003.

[685] Ley 8/2012, de 28 de diciembre, de Medidas Fiscales y Administrativas de la Comunidad de Madrid. BOCM de 29.12.2012. Artículo 61.
La supresión de la Agencia de Protección de Datos de Madrid fue una medida controvertida. Se llevó a cabo en el marco de ajustes presupuestarios del sector público, entendiendo que las funciones que realizaba el organismo podían ser asumidas por la Agencia Española de Protección de Datos, suponiendo un ahorro de costes de aproximadamente dos millones de euros.

creados o gestionados por la Administración Local del ámbito territorial de la Comunidad Autónoma de que se trate.

Con posterioridad a la LOPD se crearon las agencias de Cataluña y País Vasco.

La ley 5/2002 de la Agencia Catalana de Protección de Datos[686] crea la Autoridad de control para Cataluña, siendo aprobando su Estatuto por el Decreto 48/2003[687]. La aprobación del Estatuto de Autonomía de Cataluña en 2006 en el que se reconocía por vez primera en el ámbito estatutario el derecho a la protección de datos, llevó a la aprobación de la ley 32/2010 de la Autoridad Catalana de Protección de Datos[688], por la que se modificaba la denominación del organismo, pasando a llamarse Autoridad Catalana de Protección de Datos[689].

Mediante la ley 2/2004, del Parlamento Vasco, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de creación de la Agencia Vasca de Protección de Datos[690] se crea la Autoridad de control del País Vasco.

La Comunidad Autónoma de Andalucía también ha creado su propio organismo de control en materia de protección de datos en la figura del Consejo de Transparencia y Protección de Datos de Andalucía a través de la aprobación de la Ley 1/2014, de Transparencia Pública de Andalucía[691]. Dicho organismo no está exento de controversias en tanto que en una misma autoridad confluye el control en materia de protección de datos y de transparencia. Por Decreto 434/2015 se han aprobado los Estatutos del Consejo[692].

---

[686] Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos.
DOGC núm. 3625, de 29.04.2002 y BOE núm. 115, de 14.05.2002.

[687] Decreto 48/2003, de 20 de febrero, por el cual se aprueba el Estatuto de la Autoridad Catalana de Protección de Datos.

[688] Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos.
DOGC núm. 5731 de 08.10.2010 y BOE núm. 257 de 23.10.2010.

[689] Según recoge acertadamente el Preámbulo de la ley, el cambio de denominación se hizo *"para evitar la confusión de su naturaleza con el de las entidades de carácter instrumental que bajo la denominación de agencias han aparecido últimamente en el ámbito administrativo".*

[690] Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.
BOPV núm. 44, de 4.03.2004 y BOE núm. 279, de 19.11.2011.

[691] Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía.
BOJA núm. 124 de 30.06.2014 y BOE núm. 172, de 16.07.2014.

[692] Decreto 434/2015, de 29 de septiembre, por el que se aprueban los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía. BOJA núm. 1933, de 2.10.2015.

Otras comunidades autónomas han hecho amagos varios de creación de autoridades de control autonómicas, si bien no han terminado de fraguarse. Ha habido proyectos en Valencia, Castilla-la Mancha y Galicia.

El artículo 41.3 recoge el deber de cooperación y coordinación entre las autoridades de control autonómicas y la Agencia Española de Protección de Datos[693]. En este mismo sentido el artículo 64 del Real Decreto 1720/2007, de desarrollo de la LOPD, recoge explícitamente la colaboración en lo que respecta a los ficheros[694].

4.4.2 Funciones.

Con la Ley Orgánica de Protección de Datos de 1999, el reconocimiento a los órganos autonómicos se plasma, tal como hemos comentado, en el artículo 41 de la misma, por el que los dota de las mismas funciones de la Agencia Española de Protección de Datos, a excepción de las recogidas en los apartados j), k) y l) del artículo 37: velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine; redactar una memoria anual y remitirla al Ministerio de Justicia y ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

Delimitadas las funciones que no podrán realizar, sí serán funciones de las autoridades autonómicas las siguientes:

[693] Art. 41.3 LOPD: *"El Director de la Agencia de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. El Director de la Agencia de Protección de Datos y los órganos correspondientes de las Comunidades Autónomas podrán solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones".*

[694] Artículo 64 RD 1720/2007**.** *Colaboración con las autoridades de control de las comunidades autónomas: "El Director de la Agencia Española de Protección de Datos podrá celebrar con los directores de las autoridades de control de las comunidades autónomas los convenios de colaboración o acuerdos que estime pertinentes, a fin de garantizar la inscripción en el Registro General de Protección de Datos de los ficheros sometidos a la competencia de dichas autoridades autonómicas".*

- Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
- Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.
- Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la ley.
- Atender las peticiones y reclamaciones formuladas por las personas afectadas.
- Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.
- Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.
- Ejercer la potestad sancionadora en los términos previstos por el Título VII de la ley.
- Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrolle la ley.
- Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

Asimismo el artículo 41 LOPD les reconoce la potestad sancionadora[695] y la de inmovilización de ficheros[696]. También podrán crear y mantener sus propios registros

[695] Artículo 46 LOPD.
[696] Artículo 49 LOPD.

de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos[697] con el deber de colaboración con la AEPD anteriormente expuesto.

Tal y como expone Troncoso Reigada[698], también les corresponden a las autoridades autonómicas funciones descritas en otros artículos de la LOPD, en cuanto a los ficheros creados por las Comunidades Autónomas en su ámbito de competencia. Así, serán competentes en los procedimientos de tutela de los derechos de acceso, rectificación, cancelación y oposición del artículo 18.2 LOPD[699]; en lo relativo a la excepción de esos derechos, artículo 23.3 LOPD[700]; en relación a la inscripción de los códigos tipo ya que podrán inscribirse en los registros autonómicos, artículo 32.3 LOPD[701]; en relación al ejercicio de las potestades de inspección por las autoridades de control, artículo 40.1 LOPD[702]; y en lo referente a las Resoluciones de las autoridades autonómicas que finalizan la vía administrativa en el procedimiento sancionador, artículo 48 LOPD[703].

[697] Artículo 41.2 LOPD.

[698] TRONCOSO REIGADA, A. *La Distribución competencial entre el Estado y las Comunidades Autónomas en protección de datos personales*. Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas, núm. 1, 2005 (Ejemplar dedicado a: Los derechos fundamentales y las nuevas tecnologías), p. 129.

[699] Artículo 18.2 LOPD: "El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación".

[700] Art. 23.3 LOPD: *"El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación".*

[701] Artículo 32.3 LOPD: *"Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41".*

[702] Artículo 40.1 LOPD: *"Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos".*

[703] Artículo 48 LOPD. Procedimiento sancionador: *"Las resoluciones de la Agencia de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa".*

4.4.3 Reparto competencial.

El reparto de competencias entre el Estado y las Comunidades Autónomas en materia de protección de datos ya fue abordado desde el punto de vista constitucional[704] en el que, a modo de resumen, decíamos que la competencia legislativa es del Estado así como también lo son las competencias ejecutivas sobre ficheros privados. Sin embargo, las competencias ejecutivas sobre ficheros de titularidad pública podrán ser desarrolladas por las Comunidades Autónomas cuando así lo recojan sus Estatutos y tengan la previsión normativa necesaria para llevarla a cabo.

El ámbito de aplicación de la ley difiere entre las disposiciones de unas y otras comunidades autónomas. Como dice Troncoso Reigada *"la línea divisoria entre el ámbito competencial de la Agencia Española de Protección de Datos y las Agencias Autonómicas… es la distinción entre lo público y lo privado,* siendo que *"para que la Agencia de Protección de Datos de una Comunidad Autónoma tenga competencia no basta con que sea un fichero de una Corporación de Derecho Público; es necesario que sea un fichero creado o gestionado para el ejercicio de funciones públicas"*[705]. La extinta Agencia de Protección de Datos de la Comunidad Autónoma de Madrid y la Agencia Vasca de Protección de Datos desarrollaron sus competencias en idéntico sentido, si bien la vasca fue mucho más precisa en la descripción de los organismos cuyos ficheros estarían bajo el control de la Comunidad Autónoma[706], incluyendo las Universidades Públicas, y dejando las privadas para la Agencia española.

[704] Apartado 4.1.3.
[705] Ver 691, p. 130.
[706] Artículo 2.1 Ley Vasca 2/2004: "*Artículo 2. Ámbito de aplicación. 1.–La presente ley será aplicable a los ficheros de datos de carácter personal creados o gestionados, para el ejercicio de potestades de derecho público, por: a) La Administración General de la Comunidad Autónoma, los órganos forales de los territorios históricos y las administraciones locales del ámbito territorial de la Comunidad Autónoma del País Vasco, así como los entes públicos de cualquier tipo, dependientes o vinculados a las respectivas administraciones públicas, en tanto que los mismos hayan sido creados para el ejercicio de potestades de derecho público. b) El Parlamento Vasco. c) El Tribunal Vasco de Cuentas Públicas. d) El Ararteko. e) El Consejo de Relaciones Laborales. f) El Consejo Económico y Social. g) El Consejo Superior de Cooperativas. h) La Agencia Vasca de Protección de Datos. i) La Comisión Arbitral. j) Las corporaciones de derecho público, representativas de intereses económicos y profesionales, de la Comunidad Autónoma del País Vasco. k) Cualesquiera otros organismos o instituciones, con o sin personalidad jurídica, creados por ley del Parlamento Vasco, salvo que ésta disponga lo contrario*".

Sin embargo, la Agencia catalana (hoy Autoridad de Control Catalana) ha interpretado el concepto público de una forma mucho más amplia. En relación con las universidades se atribuye también las competencias sobre los ficheros de todas las universidades del ámbito territorial de Cataluña, con lo que quedan incluidas las universidades privadas. En estos entes nos encontramos con un doble control, pues la AEPD es la encargada del procedimiento de inscripción de los ficheros (por su carácter privado) y es la Autoridad catalana quien ejerce el control posterior. También ha ampliado la Agencia catalana sus competencias en lo referente a las sociedades mercantiles. Si para la Agencia Vasca (y también lo era para la de Madrid) el criterio diferenciador para ser competente sobre los ficheros de una empresa era la naturaleza jurídica (pública o privada), la Catalana extiende sus competencias de control a todas aquellas entidades privadas que presten servicios públicos aunque no sean concesionarios de estos, así como a las empresas privadas cuando tengan participación mayoritaria de capital público, o sus ingresos presupuestarios provengan mayoritariamente de estos, o bien los órganos directivos designados por entes públicos sean mayoría[707]. A la vista del artículo 3 de la ley 32/2010 de la Autoridad Catalana de Protección de Datos, la competencia de control recaerá sobre todos aquellos ficheros que de una u otra forma tengan relación con lo público.

[707] Ley 32/2010 de la Autoridad Catalana de Protección de Datos. Artículo 3: "*Ámbito de actuación. El ámbito de actuación de la Autoridad Catalana de Protección de Datos comprende los ficheros y los tratamientos que llevan a cabo: a) Las instituciones públicas. b) La Administración de la Generalidad. c) Los entes locales. d) Las entidades autónomas, los consorcios y las demás entidades de derecho público vinculadas a la Administración de la Generalidad o a los entes locales, o que dependen de ellos. e) Las entidades de derecho privado que cumplan, como mínimo, uno de los tres requisitos siguientes con relación a la Generalidad, a los entes locales o a los entes que dependen de ellos: Primero. Que su capital pertenezca mayoritariamente a dichos entes públicos. Segundo. Que sus ingresos presupuestarios provengan mayoritariamente de dichos entes públicos. Tercero. Que en sus órganos directivos los miembros designados por dichos entes públicos sean mayoría. f) Las demás entidades de derecho privado que prestan servicios públicos mediante cualquier forma de gestión directa o indirecta, si se trata de ficheros y tratamientos vinculados a la prestación de dichos servicios. g) Las universidades públicas y privadas que integran el sistema universitario catalán, y los entes que de ellas dependen. h) Las personas físicas o jurídicas que cumplen funciones públicas con relación a materias que son competencia de la Generalidad o de los entes locales, si se trata de ficheros o tratamientos destinados al ejercicio de dichas funciones y el tratamiento se lleva a cabo en Cataluña. i) Las corporaciones de derecho público que cumplen sus funciones exclusivamente en el ámbito territorial de Cataluña a los efectos de lo establecido por la presente ley".*

Así las cosas, la diferencia en el desarrollo de la competencia ejecutiva sobre el control de los ficheros en las comunidades autónomas con autoridad de control propia es notable. Sería arriesgado tachar de inconstitucional el desarrollo competencial que la Autoridad Catalana de Protección de Datos ha asumido por mandato del legislador autonómico, pues el problema radica en la ausencia normativa absoluta de distribución competencial en esta materia por parte del constituyente. Queda a expensas de las comunidades asumir competencias interpretando conceptos. Y eso es lo que ha hecho Cataluña. Ahora bien, como comunidad proactiva que es en cuanto a asumir todas las competencias que el estado le ha ido permitiendo a lo largo de todos los gobiernos democráticos habidos en España, no es menos cierto que en ocasiones, como la que aquí analizamos, se genera un conflicto entre administraciones difícil de deslindar, y que finalmente serán los ciudadanos quienes asuman los inconvenientes generados en estas situaciones.

Y en esta confusión competencial donde cada comunidad hace lo que puede, la nueva Autoridad de protección de datos en Andalucía acaba de aprobar su Estatuto, en cuyo artículo 5, que denomina ámbito de actuación del Consejo, apartado 2 dice: *"En materia de protección de datos, y en aplicación del artículo 82 del Estatuto de Autonomía para Andalucía, el Consejo ejercerá sus competencias sobre las instituciones autonómicas de Andalucía, Administración autonómica, administraciones Locales, las universidades del sistema universitario andaluz, así como las entidades de derecho público y privado dependientes de cualquiera de ellas".*

En materia de universidades lo expuesto es claro. Serán competentes sobre las universidades públicas, ya que el sistema universitario andaluz está formado por las universidades públicas y otra serie de organismos e instituciones que contribuyen al funcionamiento del sistema[708].

[708] El Sistema Universitario Andaluz está compuesto por las diez universidades públicas que existen en la región, y por un conjunto de organismos e instituciones que contribuyen con su labor a la mejora del funcionamiento de este sistema y a la calidad de la enseñanza pública superior en Andalucía. La información está disponible en: http://www.juntadeandalucia.es/organismos/economiayconocimiento/areas/universidad/sistema-universitario.html.

En cuanto a las entidades de derecho privado dependientes de cualquiera de los organismos e instituciones públicos entendemos hecha la referencia a aquellas entidades creadas para gestionar los servicios públicos en las que no cabría la amplia interpretación llevada a cabo por la Autoridad catalana al entender en este caso perfectamente delimitado lo público de lo privado.

A la vista de lo expuesto, entendemos que el Parlamento Andaluz se ha alineado con las tesis de la Agencia Vasca.

4.4.4 El infome CORA.

El Informe sobre la reforma de las Administraciones Públicas, elaborado por la Comisión para la Reforma de las Administraciones públicas (CORA) y publicado el 21 de junio de 2013[709], incluye como medida número 1.02.004 la asunción por la Agencia Española de Protección de Datos las funciones de las Agencias de protección de datos Catalana y Vasca (las dos existentes a la fecha de publicación del informe) y la eliminación de los organismos autonómicos:

"Tras analizar el coste que determinados servicios o actividades implican para la Administración autonómica y estudiar la posibilidad de que aquellos sean prestados por un órgano estatal, con igual o mejor calidad, se plantea, que por órganos estatales, se asuman funciones realizadas por órganos autonómicos. Este es el caso de las competencias atribuidas a Tribunales de Cuentas, Agencias de Protección de Datos, Juntas Consultivas de Contratación Administrativa…"

En el apartado IV del informe, *Subcomisión de Duplicidades Administrativas 3. Propuestas de Carácter General u Horizontal*, con el título específico de *"Agencias de Protección de Datos"* (página 106) dice:

"En el momento actual, el régimen de protección de datos y la extensión de competencias de la Agencia Española de Protección Datos (AEPD) resulta uniforme

[709] Disponible en http://www.seap.minhap.gob.es/dms/es/web/areas/reforma_aapp/INFORME-LIBRO/INFORME%20LIBRO.PDF.

y único en relación con el sector público y el sector privado, con las únicas excepciones de las CC.AA. de Cataluña y País Vasco, que cuentan con sus propias Agencias de Protección de Datos, reguladas por Ley 2/2004 del Parlamento Vasco, de 25 de febrero, de Ficheros de Datos de Carácter Personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos y por Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos.

Junto con dichas Agencias existía una tercera autoridad, precisamente la más antigua en cuanto a su creación: la Agencia de Protección de Datos de la Comunidad de Madrid, regulada por Ley 8/2001, de 13 de julio de Protección de Datos de Carácter Personal, que fue suprimida en el año 2012, y cuyas competencias son ejercidas actualmente por la AEPD.

Estudiadas las funciones desempeñadas por las Agencias autonómicas y la infraestructura existente en la AEPD, ésta podría ejercer las funciones de aquellas, con el consiguiente ahorro presupuestario para las respectivas Comunidades".

La propuesta de la Comisión para la reforma de las Administraciones públicas se basa en tres supuestas ineficiencias:

1. Problemas de coordinación entre la Agencia Española de Protección de Datos y las Agencias Autonómicas.
2. Dificultades de mantenimiento de la unidad de criterio.
3. Ineficiencias derivadas de la duplicidad de costas.

La Autoridad Catalana de Protección de Datos realizó un análisis del informe CORA[710] en lo que a la supresión de las autoridades autonómicas de control se refiere, en el que desarrolla punto por punto su discrepancia con tales afirmaciones. Argumenta la inexistencia de duplicidad en Cataluña ya que existe un esquema de distribución de competencias recogido en su Estatuto que permite el reparto competencial: la Autoridad catalana actúa sobre el sector público y la AEPD sobre el sector privado. Rebate también la falta de coordinación entre la AEPD y las autoridades autonómicas de control describiendo pormenorizadamente todos los

[710] Disponible en: http://governacio.gencat.cat/web/.content/autogovern/documents/CORA/posicio_acpd_es.pdf.

mecanismos legalmente establecidos y otros que en la práctica se han ido creando y califica de "plenamente satisfactorios", acreditado todo ello con las declaraciones del propio Director de la AEPD. En cuanto al mantenimiento de la unidad de criterio, la autoridad catalana explica que es una conclusión sin ningún análisis que la justifique y que existen mecanismos incluso a nivel internacional –Grupo de Trabajo del artículo 29- para coordinar respuestas de las Autoridades de control ante las nuevas realidades tecnológicas. Por último, discrepa también en lo relativo a las ineficiencias derivadas de los costes, y entiende que el análisis presentado es erróneo porque extrapola la situación con la comunidad de Madrid que es bien distinta en territorio, fija un tiempo de referencia en el análisis que no es representativo, las funciones analizadas no son todas y además no se tiene en cuenta el incremento de recursos económicos que la AEPD necesitaría para asumir las competencias. Pero realmente el punto más importante sobre el que enfatiza la Autoridad catalana es el aspecto competencial, pues las competencias de Cataluña en protección de datos son mayores que las de Madrid.

Por último, existe además un punto importante a tener en cuenta. Cataluña tiene sus competencias en materia de protección de datos asumidas en su Estatuto, por lo que la atribución de sus competencias a la AEPD sería ilegal. Para llevar a cabo tal asunción de competencias debería existir una reforma estatutaria previa.

No es este el caso del País Vasco que realmente no tiene las competencias en materia de protección de datos asumidas en su Estatuto, por lo que en ese caso, al menos jurídicamente, sí sería posible llevar a cabo la reducción del organismo.

En cuanto a la estructura institucional creada en España para el ejercicio de las competencias debidas en materia de protección de datos, en 2009 se realizó un estudio[711] con una serie de modelos econométricos que pretendía proporcionar un análisis sobre la incidencia y efectividad de las autoridades de protección de datos en la aplicación y cumplimiento del derecho a la protección de datos. Dicho informe concluía que "*a pesar de la complejidad del reparto competencial entre Agencias, la*

[711] LÓPEZ ROMÁN, E. y MORA, J. *Un análisis de la estructura institucional de protección de datos en España*. INDRET. Revista para el análisis del Derecho, núm. 2. 2009. Disponible en: http://www.indret.com/pdf/641_es.pdf.

estructura institucional que poseemos sí se muestra efectiva para la promoción y defensa del derecho a la autodeterminación informativa… En otras palabras, la acción de las Agencias parece reforzarse en su actuación conjunta, lejos de revertir o debilitar la protección de datos en España".

4.4.5 La Autoridad Catalana de Protección de Datos.

Está regulada en la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos.

Cataluña tiene asumidas expresamente las competencias ejecutivas en materia de protección de datos, tal y como se recoge en el artículo 156 de su Estatuto de Autonomía[712].

Su naturaleza y estructura es muy similar a la AEPD. Se define como una institución de derecho público, con personalidad jurídica propia y plena capacidad de obrar para el cumplimiento de sus fines, con plena autonomía orgánica y funcional, que actúa con objetividad y plena independencia de las administraciones públicas en el ejercicio de sus funciones[713].

[712] Estatuto de Autonomía de Cataluña. Ley Orgánica 6/2006, de 19 de julio, de reforma del Estatuto de Autonomía de Cataluña. BOE núm. 172 de 20.07.2006.
Artículo 156. *"Protección de datos de carácter personal. Corresponde a la Generalitat la competencia ejecutiva en materia de protección de datos de carácter personal que, respetando las garantías de los derechos fundamentales en esta materia, incluye en todo caso: a) La inscripción y el control de los ficheros o los tratamientos de datos de carácter personal creados o gestionados por las instituciones públicas de Cataluña, la Administración de la Generalitat, las administraciones locales de Cataluña, las entidades autónomas y las demás entidades de derecho público o privado que dependen de las administraciones autonómica o locales o que prestan servicios o realizan actividades por cuenta propia a través de cualquier forma de gestión directa o indirecta, y las universidades que integran el sistema universitario catalán. b) La inscripción y el control de los ficheros o los tratamientos de datos de carácter personal privados creados o gestionados por personas físicas o jurídicas para el ejercicio de las funciones públicas con relación a materias que son competencia de la Generalitat o de los entes locales de Cataluña si el tratamiento se efectúa en Cataluña. c) La inscripción y el control de los ficheros y los tratamientos de datos que creen o gestionen las corporaciones de derecho público que ejerzan sus funciones exclusivamente en el ámbito territorial de Cataluña. d) La constitución de una autoridad independiente, designada por el Parlamento, que vele por la garantía del derecho a la protección de datos personales en el ámbito de las competencias de la Generalitat".*

[713] Artículo 2 ley 32/2010.

Está formada por el Director y el Consejo Asesor. De la Dirección dependen las siguientes unidades: Secretaría General, Asesoría jurídica, Registro de Protección de Datos e Inspección.

Según el artículo 7 de la ley 32/2010 la Directora actúa con sujeción al ordenamiento jurídico, con plena independencia y objetividad y sin sujeción a mandato imperativo alguno ni a instrucción de ninguna clase. Es nombrada por mayoría cualificada (tres quintos) del Parlamento. Si bien estas características junto con el sistema de incompatibilidades descritas en la norma revelan a priori la independencia, entendemos que esta no es total si la remoción puede ser acordada por el Parlamento.

4.4.6 Agencia de Protección de Datos Vasca.

Es creada al amparo de la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de creación de la Agencia Vasca de Protección de Datos, y en 2005 se aprueba su Estatuto mediante el Decreto 309/2005, de 18 de octubre.

El Estatuto de Autonomía del País Vasco[714] es del año 1979 y aún no ha sido reformado, por lo que las competencias en materia de protección de datos no están recogidas en el mismo.

El artículo 1 de la ley 2/2004 la define como un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las administraciones públicas en el ejercicio de sus funciones, si bien el Director es nombrado y cesado por disposición acordada por el Gobierno Vasco.

Su estructura también es similar a la AEPD. Está formada por un Director y un Consejo Consultivo. Del Director dependen jerárquicamente el Registro y Auditoría

[714] Ley Orgánica 3/1979, de 18 de diciembre, de Estatuto de Autonomía para el País Vasco. BOE núm. 306, de 22.12.1979.

de Protección de Datos y las áreas de asesoría jurídica, inspección y Secretaría general.

4.4.7 El Consejo de Transparencia y Protección de Datos de Andalucía.

4.4.7.1 Base legal.

El Consejo ha sido creado por la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía, habiendo siendo aprobado su Estatuto por Decreto 434/2015 de 29 de septiembre.

En el año 2003 se presentó un proyecto de ley para la creación de una Agencia Andaluza de Protección de Datos[715] que se admitió a trámite pero finalmente no salió adelante.

El Estatuto de Autonomía de Andalucía de 1981, al igual que otros coetáneos, no mencionaba la competencia en materia de protección de datos. Fue en el nuevo Estatuto de Autonomía de Andalucía, aprobado por Ley Orgánica 2/2007[716], donde se recoge en el artículo 82 la competencia ejecutiva para Andalucía en esta materia: *"Corresponde a la Comunidad Autónoma de Andalucía la competencia ejecutiva sobre protección de datos de carácter personal, gestionados por las instituciones autonómicas de Andalucía, Administración autonómica, Administraciones locales, y otras entidades de derecho público y privado dependientes de cualquiera de ellas, así como por las universidades del sistema universitario andaluz."*

Pero Andalucía no ha desarrollado normativamente su competencia (como tampoco lo ha hecho en otros ámbitos normativos como el suelo o vías pecuarias), sino que directamente ha creado un órgano para ejercerla. No ha sido así en el caso de las otras tres comunidades que han tenido agencia de protección de datos autonómica.

[715] Proposición de Ley de creación de la Agencia Andaluza de Protección de Datos presentada por el Grupo Parlamentario Popular de Andalucía. BOPA núm. 569, de 14.10.2003.
[716] Ley Orgánica 2/2007, de 19 de marzo, de reforma del Estatuto de Autonomía para Andalucía. BOE núm. 68, de 20.03.2007.

Como hemos apuntado anteriormente, la Agencia de Madrid se crea al amparo de la ley 13/1995, de regulación del uso de la informática en el tratamiento de datos personales; la Agencia catalana lo hace en la Ley 5/2002 de la Agencia Catalana de Protección de Datos; y la Agencia vasca a través de la Ley 2/2004 de Ficheros de Datos de Carácter Personal de Titularidad Pública y de creación de la Agencia Vasca de Protección de Datos.

4.4.7.2 Protección de datos y transparencia.

La ley 1/2014 creó el Consejo de Transparencia y Protección de Datos de Andalucía en su artículo 43[717]. El gobierno andaluz ha considerado agrupar en el mismo órgano las competencias en materia de protección de datos y de transparencia[718]. No es este el modelo seguido en España ni a nivel central ni por ninguna otra comunidad autónoma, pero sí los hay en el derecho comparado. En la Unión Europea solamente el Reino Unido tiene un organismo de supervisión similar, el *Information Commissioner´sOffice* (ICO)[719], encargado de controlar la aplicación de la legislación en materia de protección de datos y la relativa a la libertad de información prevista en la Ley de Libertad de Información (FOIA), que regula el

[717] Artículo 43 Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía: *"Se crea el Consejo de Transparencia y Protección de Datos de Andalucía, en adelante el Consejo, como autoridad independiente de control en materia de protección de datos y de transparencia en la Comunidad Autónoma de Andalucía".*

[718] El gobierno español aprobó la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. BOE núm. 295, de 10.12.2013, normativa de carácter básico.

[719] La Oficina del Comisionado de información (ICO) es el órgano público independiente del Reino Unido establecido para fomentar el acceso a la información oficial y proteger la información personal. Lleva a cabo este cometido promocionado prácticas recomendables, dictaminando en quejas que reúnen las condiciones exigidas, proporcionando información a personas físicas y organizaciones y tomando las medidas adecuadas cuando se infringe la ley.
ICO se encarga de hacer cumplir y supervisar la Ley de Protección de Datos, la Ley de Libertad de Información, las Regulaciones para la Información Medioambiental y las Regulaciones de Comunicaciones Electrónicas.
Sus funciones principales son, según su propia información facilitada en su web, educar e influenciar (promueven prácticas recomendables y facilitan información y asesoramiento), resolver problemas (resuelven quejas que reúnen las condiciones exigidas de personas que consideran que les han violado sus derechos) y hacer respetar las obligaciones (imponer sanciones legales contra quienes las ignoran o se niegan a aceptarlas).
La información de la ICO está disponible en: https://ico.org.uk/.

acceso a los datos personales que obran en el sector público.[720] Fuera de nuestras fronteras, en México, el órgano de control de transparencia ha asumido las competencias en materia de protección de datos personales. Es el INAI -Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales-.[721]

La decisión de elegir este modelo de unificación la argumenta la propia Exposición de Motivos de la ley 1/2014 al referirse a la *"evidente interconexión entre ambas materias",* consiguiéndose una "*economía organizativa y la coherencia en la aplicación de los criterios que deben regir… cuando facilitan información pública a la ciudadanía*".

Consideramos acertada la voluntad del legislador de desarrollar las competencias en materia de protección de datos, si bien la configuración de la Autoridad de control con materias compartidas quizás pueda generar, el tiempo lo dirá, un grado de ineficiencia del organismo en cuestión. En las mencionadas argumentaciones vertidas en la Exposición de Motivos, dar coherencia en la aplicación de los criterios no parece una razón lógica por la que unir dos organismos que tienen funcionalidades distintas. Si bien es cierto como decíamos que el equilibrio entre el derecho de acceso a la información y el derecho a la protección de datos tiene unos límites muy finos, ello no supone que las funciones a desempeñar por quien protege cada uno de esos derechos sean similares. De hecho, el propio artículo 45 de la ley 1/2014 dice que el Consejo actuará en materia de protección de datos en los términos previstos en el artículo 41 de la LOPD, y como garante del derecho a la transparencia conforme a lo previsto en la Ley de Transparencia andaluza y en la legislación básica de la materia. Entendemos sería más eficaz articular un mecanismo similar al existente a nivel estatal, donde existen dos órganos independientes que se coordinan ante situaciones determinadas en las que ambos derechos confluyen y es complicado determinar los límites de uno y otro. Y de hecho así es como los propios Estatutos del Consejo han configurado esta relación hasta que se produzca la asunción efectiva del ejercicio de las competencias en materia de protección de datos. En su

[720] Sobre la Ley de Protección de Datos inglesa, JAY, R/HAMILTON, A: *Data protection. Law and practice*, 2ª ed., Sweet & Maxwell, Londres, 2003 (en especial, p. 518 y 534-536).
[721] Más información disponible en http://inicio.inai.org.mx/SitePages/ifai.aspx.

disposición transitoria tercera establece que en ese periodo *"el Consejo y la Agencia Española de Protección de Datos podrán adoptar en el ámbito de la cooperación institucional los criterios de aplicación, en su ámbito de actuación, de las reglas contenidas en el artículo 15 de la ley 19/2013, de 9 de diciembre, en particular en lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados cuyos datos se contuviesen en la misma, de conformidad con lo dispuesto en dicha Ley y en la Ley Orgánica 15/1999, de 13 de diciembre".*

El otro razonamiento dado en la Exposición de Motivos acerca de la oportunidad de crear un único organismo es de carácter económico. Pues bien, no podemos compartir dicha justificación, y ello por dos razones:

La primera porque una Autoridad de control en materia de protección de datos autonómica es prescindible, y máxime en la coyuntura económica en la que se hayan España y Andalucía, por lo que su gasto en el momento actual es innecesario e injustificado. Sus competencias están siendo ejercidas por el organismo estatal, la Agencia Española de Protección de Datos. Por lo tanto no hay razón para tener que crear un nuevo organismo en esta materia.

La segunda porque el organismo que ejerza las competencias en materia de transparencia puede ser un organismo ya existente en la Junta de Andalucía que asuma nuevas competencias. Andalucía tiene un despliegue más que importante de Comisiones, Comités, Consejos y órganos en general en materia de documentación que pueden aglutinar perfectamente las competencias del recién creado Consejo de Transparencia. Como decíamos, la finalidad del órgano en materia de transparencia es ser "garante del derecho a la transparencia", y tal derecho consiste en "facilitar el conocimiento a la ciudadanía de la actividad de los poderes públicos y de las entidades con financiación pública", y ello se hace a través de la publicidad activa y del derecho de acceso a la información pública[722]. Ambos conceptos, publicidad activa e información pública vienen definidos en el artículo 2 de la ley[723].

[722] Artículo 1 Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía: "*Artículo 1. Objeto.*

Pues bien, el derecho de acceso a la información pública no es nuevo. Como referencia, a nivel estatal, la Constitución ya lo recogió como tal derecho en el artículo 105 bis[724], también los artículos 35.h y 37 de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común[725] y la ley 11/2007[726], de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos[727]; a nivel europeo el derecho de acceso está recogido en el artículo 42 de la Carta de los Derechos Fundamentales del año 2000[728]; pero a nivel autonómico, Andalucía ha sido pionera en elaboración de normativa al respecto. Así, la ley 3/84 de Régimen de Archivos de Andalucía, desarrollada por el Decreto 73/1994, de 29 de marzo, que aprueba el Reglamento de Organización del Sistema Andaluz de

La presente ley tiene por objeto la regulación, en el ámbito de la Comunidad Autónoma de Andalucía, de la transparencia en su doble vertiente de publicidad activa y de derecho de acceso a la información pública, como instrumento para facilitar el conocimiento por la ciudadanía de la actividad de los poderes públicos y de las entidades con financiación pública, promoviendo el ejercicio responsable de dicha actividad y el desarrollo de una conciencia ciudadana y democrática plena".

[723] Ídem. Artículo 2: *"A los efectos de la presente ley, se entiende por: a) Información pública: los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguna de las personas y entidades incluidas en el presente título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones. b) Publicidad activa: la obligación de las personas y entidades a las que hacen referencia los artículos 3 y 5 de hacer pública por propia iniciativa, en los términos previstos en la presente ley, la información pública de relevancia que garantice la transparencia de su actividad relacionada con el funcionamiento y control de su actuación pública".*

[724] Constitución Española. Artículo 105: *"La ley regulará b) El acceso de los ciudadanos 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".*

[725] Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. BOE núm. 285, de 27.11.1992.
Artículo 35: *"Los ciudadanos, en sus relaciones con las Administraciones Públicas, tienen los siguientes derechos: h) Al acceso a la información pública, archivos y registros".*
Artículo 37: "Los ciudadanos tienen derecho a acceder a la información pública, archivos y registros en los términos y con las condiciones establecidas en la Constitución, en la Ley de transparencia, acceso a la información pública y buen gobierno y demás leyes que resulten de aplicación".

[726] Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos BOE núm. 150, de 23.06.2007.

[727] Sobre el desarrollo de la ley 11/2007, ver SÁNCHEZ BLANCO, A. *La ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos y su significativa proyección sobre el sistema de archivo*. Revista TRIA, núm. 15, 2009, p. 137-160; CRUCES BLANCO, E. *El acceso a la información, a la documentación y a los archivos. Acceso y gestión documental en la Ley 7/2011, de 3 de noviembre, de Documentos, Archivos y Patrimonio Documental de Andalucía*. Revista TRIA, núm. 17, 2011, p. 143-172.

[728] Carta de los Derechos Fundamentales. Artículo 42: *"Derecho de acceso a los documentos. Todo ciudadano de la Unión o toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro tiene derecho a acceder a los documentos del Parlamento Europeo, del Consejo y de la Comisión".*

Archivos, o la ley 7/2011, de 3 de noviembre, de documentos, archivos y patrimonio documental de Andalucía[729].

En el desarrollo de esta última ley, se crea la Comisión Andaluza de Valoración y Acceso a los Documentos como órgano ejecutivo, y la Comisión del Sistema Archivístico de Andalucía como órgano consultivo. Ambas comisiones son un ejemplo de órganos que podrían asumir dichas competencias. Creada la primera por la ley 7/2011, de Documentos, Archivos y Patrimonio Documental de Andalucía[730] es un órgano colegiado y de participación, formado por trece técnicos, al que corresponde la valoración de los documentos de titularidad pública y la aplicación de su régimen de acceso[731]. Como órgano ejecutivo que es, completa su actividad con un órgano consultivo como es la Comisión del Sistema Archivístico de Andalucía, creada también por la ley 7/2011[732] entre cuyas funciones está actuar como órgano de información, consulta y asesoramiento del Sistema Archivístico de Andalucía[733].

4.4.7.3 Estructura y naturaleza jurídica.

El artículo 1 de los Estatutos del Consejo define a este como *"la autoridad independiente de control en materia de transparencia y protección de datos en la comunidad Autónoma de Andalucía"*. *"El Consejo se configura como una entidad pública con personalidad jurídica propia, con plena capacidad y autonomía orgánica y funcional para el ejercicio de sus cometidos".*

[729] Sobre el análisis de la ley 7/2011, CRUCES BLANCO, E. *El acceso a la información, a la documentación y a los archivos. Acceso y gestión documental en la Ley 7/2011, de 3 de noviembre, de Documentos, Archivos y Patrimonio Documental de Andalucía.* Revista TRIA, núm. 17, 2011, p. 143-172.

[730] La Comisión Andaluza de Valoración y Acceso a los Documentos hereda la composición y funcionamiento de la Comisión Andaluza Calificadora de Documentos Administrativos, creada por decreto 97/2000, de 6 de marzo por el que se aprueba el Reglamento del Sistema Andaluz de Archivos.

[731] Información disponible en: http://www.juntadeandalucia.es/culturaydeporte/web/areas/archivos/sites/consejeria/areas/archivos/cavad.

[732] La Comisión del Sistema Archivístico de Andalucía hereda la composición y funcionamiento de la Comisión de Coordinación del Sistema Andaluz de Archivos, creada igualmente por el Decreto 97/2000 de 6 de marzo por el que se aprueba el Reglamento del Sistema Andaluz de Archivos.

[733] Sobre los archivos administrativos, SÁNCHEZ BLANCO, A. *Archivos estatales y archivos autonómicos.* Revista Jurídica de Navarra, julio-diciembre 2009, núm. 48, p.131-179.

En su artículo 2, denominado "independencia", dice que el Consejo ejercerá sus funciones con objetividad, profesionalidad, sometimiento al ordenamiento jurídico y plena independencia de las Administraciones Públicas en el ejercicio de las mismas.

En cuanto a su estructura, se configura como un órgano de carácter unipersonal, la Dirección, y una Comisión Consultiva como órgano de participación y consulta.

Según los Estatutos, la Dirección tiene adscritas cuatro áreas: Transparencia, Protección de Datos, Secretaría General y Asesoría Jurídica. Y además podrá crear grupos o comisiones de trabajo para mejorar la coordinación de sus actividades. Las distintas unidades ejercerán sus funciones coordinadamente, especialmente en la ponderación de los principios e intereses relacionados con la transparencia pública y la protección de datos. Establece también que el titular de la Dirección *"ejercerá sus funciones con plena independencia, neutralidad, dedicación exclusiva y objetividad, no estando sujeta a instrucción o indicación alguna en el desempeño de aquellas".* Para dotarla de mayor independencia se acordó que su designación será realizada por el Parlamento por mayoría absoluta. Deberá ser una persona de reconocido prestigio y competencia profesional, con una experiencia mínima de quince años en materias relacionadas con la administración pública y que no esté incursa en el régimen de incompatibilidades que los propios Estatutos determinan. En cuanto a las causas de expiración del puesto se prevé la posibilidad de que el Consejo de gobierno lo acuerde anticipadamente previa instrucción de expediente.

La descripción del ente así como de las características del titular de la Dirección confluyen en describir la tan predicada independencia de los organismos de control, si bien encontramos en el sistema alguna quiebra. El hecho de que la Asesoría Jurídica pueda ser encomendada al gabinete jurídico de la Junta de Andalucía hace pensar en la posibilidad de que éstas ejerzan una influencia sobre las decisiones de la Autoridad de control. De hecho, esta circunstancia planea sobre los Estatutos cuando en el apartado 6 del artículo 8 dice que cuando la representación y defensa jurisdiccional del Consejo se encomiende al Gabinete Jurídico de la Junta, mediante el correspondiente convenio, se deberá incluir una cláusula para los supuestos en los que exista contraposición de intereses. No debemos olvidar que el Consejo ha de

supervisar el cumplimiento de la legalidad en protección de datos de la Administración, por lo que no podrá ésta formar parte de la institución supervisora, pues la influencia está servida. Tal y como dijo el Tribunal de Justicia de la Unión Europea en el asunto de la Comisión contra la República Federal de Alemania en el asunto de las autoridades de control de los *länder* alemanes, *"la mera posibilidad de que las autoridades de tutela puedan ejercer influencia política sobre las decisiones de las autoridades de control es suficiente para obstaculizar el ejercicio independiente de las funciones de éstas"*[734].

Por otro lado, el artículo 7 de los Estatutos establece que el Consejo se regirá por los Estatutos y por una serie de normas entre la que destaca en el apartado b) la aplicación supletoria de la normativa aplicable a las agencias administrativas. Tal y como establece el artículo 54 de la ley 9/2007 de la Administración de la Junta de Andalucía[735]"*las agencias son entidades con personalidad jurídica pública dependientes de la Administración de la Junta de Andalucía para la realización de actividades de la competencia de la Comunidad Autónoma en régimen de descentralización funcional".* En la medida en que los Estatutos del Consejo asimilan, aunque sea supletoriamente, su régimen jurídico al de las Agencias demuestra una estructura organizativa dependiente.

En cuanto a la Comisión Consultiva de la Transparencia y la Protección de Datos, se define en el artículo 12 de los Estatutos como un órgano colegiado de participación y consulta en Andalucía en materia de transparencia pública y protección de datos. Es un órgano similar a los existentes en otras autoridades de control, si bien su composición es probablemente excesiva, pues está formada por catorce miembros, el número más alto con diferencia de entre todos los órganos en España con competencias en materia de transparencia.

[734] Sentencia TJUE (Gran Sala) de 9.03.2010. Asunto C-518/07. Comisión Europea vs República Federal de Alemania.

[735] ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía. BOJA núm. 215 de 31.10.2007.

4.4.7.4 El reto.

Inicialmente, en el año 2014 cuando se creó el Consejo de Transparencia y Protección de Datos, la dotación presupuestaria para el ejercicio 2015 fue de 60.000 €[736], una cantidad irrisoria para un organismo de la envergadura del nuevo Consejo. El presupuesto para el ejercicio 2016 recoge una partida de 1.241.806 €[737], un importe razonable si lo ponemos en relación con el de las otras comunidades autonómicas, aunque inferior.

Según los datos de la Memoria de 2014 de la Agencia Española de Protección de Datos, a 31 de diciembre de 2014, la administración autonómica de Andalucía tenía inscritos 1952 ficheros (es la tercera comunidad con mayor número de ficheros inscritos, por detrás de Madrid y Cataluña) y la administración local 10.756. Esto hace un total de 12.708 ficheros a los que habría que añadirle los inscritos en el año 2015 más todos los pertenecientes a personas jurídico públicas cuyos datos no aparecen categorizados por comunidades autónomas en la Memoria. Este será parte del trabajo inicial que el nuevo Consejo tendrá que asumir, el traspaso para su control y seguimiento de más de trece mil ficheros. A partir de aquí tendrá que desarrollar todas las competencias que supone el Registro de los ficheros: mantenimiento logístico del Registro, atender los ejercicios de los derechos ARCO por los ciudadanos, atender las modificaciones y cancelaciones de los ficheros existentes, inscribir los nuevos, ejercer la potestad inspectora y sancionadora, etc. Pero donde realmente aporta valor a sus ciudadanos una Autoridad de control es en el ejercicio de difusión de la cultura de la protección de datos y en el asesoramiento a ellos. Tendrá que estar presente en cuantos foros nacionales e internacionales pueda.

Deberá además el Consejo estar a las novedades legislativas que marque Bruselas con el Reglamento General de Protección de Datos. Las nuevas obligaciones que detallábamos en el apartado 4.3.4 que recaerán sobre las Autoridades de control nacionales también le serán de aplicación en su mayoría a las autoridades

[736] Disponible en: http://www.juntadeandalucia.es/economiayhacienda/planif_presup/presupuesto2015/estado/programas/tomo1_2.pdf.

[737] Disponible en: http://www.juntadeandalucia.es/haciendayadministracionpublica/planif_presup/proy_presupuesto2016/estado/servicios/servicios-b-7.pdf.

autonómicas, y si decíamos que la Agencia española tendrá que dotar muchos y nuevos recursos para afrontar las nuevas competencias, el Consejo de Transparencia y Protección de Datos de Andalucía los tiene que dotar todos. La ley fue aprobada en el Parlamento por unanimidad. Las expectativas son muchas. El trabajo que comienza el nuevo Consejo es duro y difícil, pero a la vez un gran reto ilusionante con miras al desarrollo y a la democracia en Andalucía.

5 Conclusiones.

Estableceremos las conclusiones en tres ámbitos: Europa, España y Andalucía, si bien con carácter genérico hay una conclusión que alcanza a todos: la normativa en protección de datos y las Autoridades de Control en todos los niveles no cumplirán sus objetivos si no aumenta la conciencia de los ciudadanos sobre el derecho a la protección de datos, cómo ejercerlo y cómo garantizarlo. Se hace necesario predicar más activamente una cultura de protección de datos desde todas las instancias. La labor preventiva ha de ser la gran aportación por parte de las autoridades de ámbito regional.

5.1 Respecto de Europa.

1. La revisión del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y el nuevo Reglamento Europeo de Protección de Datos están totalmente alineados. Se pretende una armonización normativa en toda Europa.

2. El nuevo Reglamento General de Protección de Datos emplea conceptos jurídicos indeterminados que previsiblemente supondrán un desbordamiento tanto de las instancias judiciales como de las Autoridades de control. Se hacen necesarias directrices vinculantes para la interpretación de las mismas.

3. El mecanismo de coherencia descrito en el nuevo Reglamento General de Protección de Datos deberá simplificarse, dotando de personalidad jurídica al Consejo Europeo de Protección de Datos para que sus decisiones sean vinculantes y efectivas.

4. Para la armonización real en la normativa y aplicación del derecho a la protección de datos debe existir una Autoridad de control jerárquicamente

superior, organismo colegiado que aúne a las Autoridades de control estatales y al Supervisor Europeo, que pueda desarrollar, coordinar y ejecutar una política común entre las Autoridades de control, especialmente en materia de transferencia internacional de datos. También deberá ejercer la supervisión sobre las Autoridades de control nacionales. Ese organismo debe ser el Consejo Europeo de Protección de Datos.

5. El nuevo Reglamento General de Protección de Datos no es de aplicación a la Administración europea. Esta cuestión deberá modificarse en el texto final o bien será necesaria la reforma urgente del Reglamento (CE) núm. 45/2001 del Parlamento Europeo y del Consejo que unifique la aplicación de la normativa en todas las instancias de la Unión Europea y a todas las Autoridades de control por igual.

6. Con la entrada en vigor del nuevo Reglamento General de Protección de Datos se dará una duplicidad en algunas funciones que están previstas desarrolle el Consejo Europeo de Protección de Datos y que actualmente también desempeña el Supervisor Europeo de Protección de Datos. El deslinde de funciones es preciso, para lo que se podría aprovechar el cambio normativo si se produce.

7. El Supervisor Europeo de Protección de Datos y el Supervisor Adjunto comparten estatus y funciones en el desempeño de su trabajo, donde existe un reparto de roles. Nos encontramos ante un caso de bicefalia en el que el poder se compensa y se hace del consenso una estrategia para la gobernanza.

8. En cuanto a los parámetros que describen la cualidad de la independencia de las Autoridades de control, deberían incluirse que la reelección del cargo no sea posible, y que la designación del órgano sea parlamentaria con mayoría cualificada.

9. La situación actual tras la invalidación del Acuerdo de Puerto Seguro de transferencia internacional de datos personales entre la Unión Europea y EEUU supone un obstáculo al desarrollo económico. Es imprescindible

buscar acuerdos inmediatos entre ambas partes para validar un sistema que garantice el cumplimiento por parte de EEUU del ejercicio del derecho a la protección de datos en términos similares a la normativa de la Unión Europea en los tratamientos de datos personales que se realicen fuera del territorio de la Unión, siendo recomendable la firma por parte de EEUU del Convenio 108 del Consejo de Europa.

5.2 Respecto de España.

10. El derecho a la protección de datos de carácter personal ha de estar recogido explícitamente como derecho fundamental en la Constitución Española.
    Se hace preciso modificar el artículo 18.4 suprimiendo el texto actual, que hace referencia obsoletamente al uso de la informática, por uno nuevo, cuyo contenido pudiera ser el siguiente:
    1. "El Estado garantizará a los españoles el derecho a la protección de datos de carácter personal que le conciernan.
    2. Se regulará por ley la protección a las personas físicas respecto del tratamiento de datos de carácter personal.
    3. La vigilancia y el cumplimiento de estas normas quedarán sujetos al control de una autoridad totalmente independiente".

11. El reparto competencial en lo referente al derecho a la protección de datos debe estar recogido explícitamente en la Carta Magna. Se deberá incluir una nueva materia en la que el Estado tiene competencia exclusiva.
    Así, el artículo 149 añadirá la materia número 33ª, que deberá decir:

    > "Legislación básica sobre protección de datos de carácter personal así como la competencia ejecutiva sobre los ficheros y tratamientos del sector privado y de todos aquellos públicos y privados en los que exista una transferencia internacional de datos".

12. Completando el marco constitucional, el artículo 148 de la Constitución española deberá recoger las competencias cedidas a las Comunidades autónomas en materias de protección de datos, añadiendo la materia número 23ª, que deberá decir:

    "La competencia ejecutiva sobre los ficheros y tratamientos del sector público".

13. Para lograr la independencia total, el Director de la Agencia Española de Protección de Datos debe ser propuesto por el Parlamento con mayoría cualificada.

14. El nuevo Reglamento General de Protección de Datos va a suponer un cambio total en las garantías y cumplimientos debidos en el ejercicio del derecho a la protección de datos. Las Autoridades de control tendrán muchos y nuevos cometidos que les obligarán a reforzar sus recursos técnicos, económicos y humanos. El tiempo de adaptación será de dos años. Se hace imprescindible acometer desde ya por la Agencia Española de Protección de Datos todas las medidas de índole técnica y organizativa necesarias para poder cumplir con las nuevas funciones de forma satisfactoria.

15. Una vez aprobado el nuevo Reglamento General de Protección de Datos se hará necesaria en España la modificación de la Ley Orgánica de Protección de Datos o bien la aprobación de una nueva ley.

5.3 Respecto de Andalucía.

16. La creación de una Autoridad de control autonómica en materia de protección de datos en Andalucía, llámese Consejo o Agencia es, en principio, plausible, pues dota de mayor contenido y estabilidad la distribución competencial en Andalucía.
17. Sin embargo, la creación del Consejo de Transparencia y Protección de Datos por la ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía, no está justificada por el momento coyuntural económico que vive la

comunidad, pues no es el idóneo para crear un nuevo organismo que requiere de un gran esfuerzo económico y cuyas funciones pueden ser desarrolladas por otros.

18. En materia de protección de datos, una Autoridad de control autonómica es ahora mismo prescindible, ya que sus funciones están llevándose a cabo por un organismo de carácter estatal como es la Agencia Española de Protección de Datos, no suponiendo ello ningún perjuicio ni coste adicional para el ciudadano.

19. En cuanto a las nuevas competencias a desarrollar y ejecutar en materia de transparencia pueden ser asumidas plenamente por organismos autonómicos ya existentes, formados por expertos, tales como la Comisión Andaluza de Valoración y Acceso a los Documentos como órgano ejecutivo, y la Comisión del Sistema Archivístico de Andalucía como órgano consultivo, a cuyos efectos habría que proceder a las modificaciones legislativas oportunas para que los mismos asumieran las nuevas competencias no descritas en sus actuales normativas.

20. El modelo de Consejo, tal y como está implantado en la Ley de Transparencia Andaluza, quiebra la independencia. Se hace necesario que la Autoridad de control en protección de datos esté totalmente desvinculada de los poderes políticos, no tenga dependencia funcional ni dependencia organizativa, para lo que habría que modificar el Estatuto del Consejo de Transparencia y Protección de Datos.

21. La Comunidad Autónoma de Andalucía ha asumido la competencia ejecutiva en materia de protección de datos en el artículo 82 de su Estatuto, y ha creado una Autoridad de control para el cumplimiento de la normativa en esta materia. Sin embargo, la Junta de Andalucía no ha previsto norma alguna que desarrolle estas competencias. Si el Consejo de Transparencia y Protección de Datos continua, el Parlamento andaluz debería aprobar una norma básica que determine cuál es el ámbito subjetivo de sus competencias en protección de datos de carácter personal.

6 Jurisprudencia.

TRIBUNAL EUROPEO DE DERECHOS HUMANOS

- Caso *Malone* contra el Reino Unido.
  Sentencia TEDH de 2 de agosto de 1984.

- Caso *Leander* contra Suecia.
  Sentencia TEDH de 26 de marzo de 1987.

- Caso *Gaskin* contra Reino Unido.
  Sentencia TEDH de 7 de julio de 1989.

- Caso Z contra Finlandia.
  Sentencia TEDH de 25 de Febrero de 1997.

- Caso I. contra Finlandia.
  Sentencia TEDH de 17 de julio de 2008.

- Caso C.C contra España.
  Sentencia TEDH de 6 de octubre de 2010.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

- Asunto C-1/58.
  Sentencia TJCE de 4 de febrero de 1959.
  Friedrich Stork & Cie contra Alta Autoridad Europea del Carbón y del Acero.
  Caso *Stork.*

- Asunto C- 13/60.
  Sentencia TJCE de 15 de julio de 1960.
  Las Sociedades mineras de la Cuenca del Ruhr y otros contra Alta Autoridad de la Comunidad Europea del Carbón y del Acero.
  Caso *Ruhrkohen-Verkaufsgesellschaften.*

- Asuntos acumulados C- 36, 37, 38 y 40/59.
  Sentencia TJCE de 15 de julio de 1960. I. *Nold* KG contra la Alta Autoridad Europea del Carbón y del Acero.
  Caso *Nold.*

- Asunto C- 40/64.
  Sentencia TJCE de 1 de abril de 1965. *Marcello Sgarlata* y otros contra la Comisión de la CEE.
  Caso *Sgarlatta.*

- Asunto C-29/69.
  Sentencia del TJCE de 12 de noviembre de 1969.
  Erich Stauder contra Stadt Ulm - Sozialamt.
  Caso *Stauder.*

- Asunto C-11/70.
  Sentencia del TJCE de 17 de diciembre de 1970.
  Internationale Handelsgesellschaft mbH contra Einfuhr- und Vorratsstelle für Getreide und Futtermittel.
  Caso *Internationale Handelsgesellschaft,*.

- Asunto C- 36/75.
  Sentencia del TJCE de 28 de octubre de 1975.
  Roland Rutili contra Ministro del Interior.
  Caso *Rutili.*

- Asunto C -62/01.
  Sentencia del TJCE, Sala Quinta, de 21/04/1994.
  Anna María Campogrande contra Comisión de las Comunidades Europeas.
  Caso Campogrande.

- Asunto C-404/92.
  Sentencia del TJCE, de 05/10/1994.
  X. contra Comisión.

- Asunto C-102/07.
  Sentencia del TJCE de 14 de octubre de 1999.
  Adidas AG y Adidas Benelux BV contra Marca Mode CV y otros. Petición de decisión prejudicial: *Hoge Raad der Nederlanden* - Países Bajos.
  Caso Adidas.

- Asunto C-372 /98.
  Sentencia del TJCE de 12 de octubre de 2000.
  The Queen and the Ministry of Agriculture contra Fischeries and Food,

- Asunto C-274/99 P.
  Sentencia del TJUE de 6 de marzo de 2001.
  Bernard Connolly contra Comisión de las Comunidades Europeas.
  Caso *Connolly*/Comisión.

- Asunto acumulados C-465/00, C-138/01 y C-139/01. Sentencia del TJUE de 20 de mayo de 2003.
  Rechnungshof contra *Österreichischer Rundfunk* y otros, (C‑465/00); *Christa Neukomm* (C‑138/01) y *Joseph Lauermann* (C‑139/01) contra *Österreichischer Rundfunk.*

- Asunto C-101/01.
  Sentencia del TJCE de 6 de noviembre de 2003.
  Procedimento penal entablado contra *Bodil Lindqvist.*
  Petición de decisión prejudicial del *Göta hovrätt* - Suecia.
  Caso *Lindqvist.*

- Asunto C-275/06.
  Sentencia del TJUE de 29 de enero de 2008.
  Promusicae contra Telefónica.
  Petición de decisión prejudicial: Juzgado de lo Mercantil nº 5 de Madrid – España.

- Asunto C-28/08 P.
  Sentencia del TJUE de 29 de junio de 2010.
  Bavarian Lager Co Ltd y la Comisión Europea.
  Caso *Bavarian Lager.*

- Asunto C-518/07.
  Sentencia del TJUE (Gran Sala) de 9 de marzo de 2010.
  Comisión Europea contra República Federal de Alemania.

- Asuntos acumulados C-92/09 y C-93/09.
  Sentencia TJUE (Gran Sala) de 9 de noviembre de 2010.
  Volker und Markus Schecke GbR (C-92/09) y *Hartmut Eifert* (C-93/09) contra *Land Hessen.*
  Peticiones de decisión prejudicial: *Verwaltungsgericht Wiesbaden* - Alemania.
  Caso *Volker und Markus Schecke y Eifert.*

- Asuntos acumulados C-468/10.
  Sentencia del TJUE de 24 de noviembre de 2011.
  Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) contra Administración del Estado.

- Asuntos acumulados C-55/11, C-57/11 y C-58/11.
  Sentencia del TJUE (sala cuarta) de 12 de julio de 2012.
  Vodafone España SA contra Ayuntamiento de Santa Amalia; Vodafone España SA contra Ayuntamiento de Tudela; y France Telecom España SA contra Ayuntamiento de Torremayor, respectivamente.

- Asuntos acumulados C-584/10 P, C-593/10 P y C-595/10 P.
  Sentencia del TJUE de 18 de julio de 2013.
  Comisión Europea y otros contra *Yassin Abdullah Kadi.*

- Asunto C-583/11 P,
  Sentencia del TJUE (Gran Sala) de 3 de octubre de 2013.
  Inuit Tapiriit Kanatami y otros contra Parlamento Europeo, Consejo de la Unión Europea, Reino de los Países Bajos y Comisión Europea.

- Asunto C-274/12 P,
  Sentencia del TJUE de 19 de diciembre de 2013.
  Telefónica SA contra Comisión Europea.

- Asuntos acumulados C-293/12 y C-594/12.
  Sentencia del TJUE (Gran Sala) de 8 de abril de 2014.
  Digital Rights Ireland Ltd contra *Minister for Communications, Marine and Natural Resources* y otros; y *Kärntner Landesregierung* y otros.
  Cuestiones prejudiciales presentadas por la *High Court* y el *Verfassungsgerichtshof*.
  Caso *Digital Rights.*

- Asunto C-288/12.
  Sentencia del TJUE de 8 de abril de 2014.
  Comisión contra Hungría.

- Asunto C-131/12.
  Sentencia del TJUE 13 de mayo de 2014 (Gran Sala).
  Google vs AEPD y Mario Costeja.
  Caso Google.

- Asunto C-212/13.
  Sentencia del TJUE de 11 de diciembre de 2014.
  František Ryneš contra *Úřad pro ochranu osobních údaju*.

- Asunto C-362/14.
  Sentencia del TJUE de 6 de octubre de 2015.
  Maximillian Schrems y *Data Protection Commissioner*.
  Caso *Schrems* / Facebook.

SENTENCIAS DEL TRIBUNAL CONSTITUCIONAL

- Sentencia del TC 76/1983, de 5 de agosto, Pleno.
  Recursos previos de Inconstitucionalidad núm. 311, 313, 314, 315 y 316/82, acumulados RI-25.
  Promovidos por Gobierno Vasco, Parlamento Vasco, Consejo Ejecutivo de la Generalidad de Cataluña, Parlamento de Cataluña y 50 diputados de las Cortes Generales.
  BOE de 18 de agosto de 1983.

- Sentencia del TC 180/1987, de 12 de noviembre.
  Recurso de Amparo número 847/1986.
  Promovido por el Ente Público RTVE.
  BOE núm. 295, de 10 de diciembre de 1987.

- Sentencia del TC 142/1993, de 22 de abril, Pleno.
  Recurso de inconstitucionalidad 190/1991.
  Promovido por 88 Senadores.
  BOE núm. 127, de 28 de mayo de 1993.

- Sentencia del TC 254/1993, de 20 de julio, Sala Primera.
  Recurso de Amparo nº 1827/1990.
  Promovido por Francisco Javier O.Z.
  BOE núm. 197 de 18 de agosto de 1993.

- Sentencia del TC 202/1999, de 8 de noviembre.
  Recurso de amparo 4.309/96.
  Promovido por don José Navarro Sánchez y otros.
  BOE núm. 300, de 16 de diciembre de 1999.

- Sentencia del TC 290/2000, de 30 de noviembre, Pleno.
  Recursos de Inconstitucionalidad 201-1993, 219-1993, 236-1993. 201/1993.
  Promovidos por el Consejo Ejecutivo de la Generalidad de Cataluña, el Defensor del Pueblo, el Parlamento de Cataluña y por don Federico Trillo- Figueroa Conde, Comisionado por 56 Diputados del Grupo Parlamentario Popular.
  BOE núm. 4, de 4 de enero de 2001.

- Sentencia del TC 292/2000, de 30 de noviembre, Pleno.
  Recurso de Inconstitucionalidad 1463/2000.
  Promovido por el Defensor del Pueblo.
  BOE núm. 4, de 4 de enero de 2001.

7 Recursos de internet.

• Artículo CNN-Expansión sobre *Safe Harbour*. Martes, 06 de octubre de 2015.	*http://www.cnnexpansion.com/tecnologia/2015/10/06/europa-invalida-acuerdo-ueeu-sobre-transferencia-de-datos*
• Consejo de Europa. *Human Rights and Rule of Law. Data Protection.*	*http://www.coe.int/t/dghl/standardsetting/DataProtection/default_en.asp.*
• Lista de los Estados parte del Convenio 108 y del Protocolo de 2001	*http://conventions.coe.int/Treaty/Commun/Cherchesig.asp?NT=108&cl=eng.*
• Lista de entidades estadounidenses adheridas a los principios de Puerto Seguro	*http://www.export.gov/safeharbor*
• Sitio del movimiento "*Europe vs Facebook"*	*http://www.europe-v-facebook.org/prism/facebook.pdf*
• Comité CAHDATA del Convenio 108.	*http://www.coe.int/t/dghl/standardsetting/dataprotection/Cahdata_en.asp*
• Acuerdos del Comité Consultivo del Convenio 108. CAHDATA. Reunión del 1 de abril de 2015.	*http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/CAHDATA%203_Report_CM(2015)40_En.pdf*
• Listado de Jurisprudencia del Tribunal Europeo de Derechos Humanos relacionado con la Protección de Datos Personales.	*http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/DP%202013%20Case%20Law_Eng%20(final).pdf*
• Organización para la Cooperación Económica y el Desarrollo (OCDE). Historia.	*http://www.oecd.org/about/history/*
• Organización para la Cooperación Económica y el Desarrollo (OCDE). Miembros y Socios.	*http://www.oecd.org/about/membersandpartners/*

• Directrices de la OCDE que regulan la privacidad y el flujo transfronterizo de datos personales (23 de septiembre de 1980)	*http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf*
• Resumen de las Directrices de la OCDE sobre protección de la privacidad y flujo transfronterizo de datos personales	*http://www.oecd.org/sti/ieconomy/15590267.pdf*
• Marco de la Privacidad de la OCDE. 2013.	*http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf*
• APEC *Cross Border Privacy Rules (CBPR) system*.	*http://www.cbprs.org/GeneralPages/About.aspx.*
• Presupuesto de la OCDE. 2015.	*http://www.oecd.org/about/budget/*
• Miembros de APEC.	*http://www.apec.org/About-Us/About-APEC/Member-Economies.aspx.*
• APEC *Privacy Framework.*	*http://publications.apec.org/publication-detail.php?pub_id=390*
• Sitio de *Trust-e,* el primer tercero certificador reconocido por APEC.	*https://www.truste.com/*
• APEC *Cross Border Privacy Rules (CBPR) system.*	*http://www.cbprs.org/Business/BusinessDetails.aspx.*
• Estados Miembros de las Naciones Unidas.	*http://www.un.org/es/members/.*
• Directrices de Naciones Unidas para la regulación de los archivos de datos personales informatizados.	*http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/organismos_internacionales/naciones_unidas/common/pdfs/D.3BIS-cp--Directrices-de-Protecci-oo-n-de-Datos-de-la-ONU.pdf.*
• *United Nations. General Assembly. The right to privacy in the digital age. 20 November 2013.*	*http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1.*
• Naciones Unidas. Asamblea General. El derecho a la privacidad en la era digital. 24 de marzo de 2015.	*http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_28_L27.pdf*

• Estándares Internacionales sobre Protección de Datos Personales y Privacidad. Resolución de Madrid. 2009.	*https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/09-11-05_Madrid_Int_standards_ES.pdf*
• Resolución sobre Big Data. *36 th International Conference of Data Protection & Privacy Commissioners*.	*http://www.privacyconference2014.org/media/16724/Resoluci%C3%B3n-Big-Data.pdf.*
• Artículo de prensa sobre la aprobación de los estándares internacionales sobre protección de datos. Eleconomista.es. 6/11/2009.	*http://www.eleconomista.es/seleccion-ee/noticias/1675918/11/09/Aprobados-unos-estandares-internacionales-sobre-proteccion-de-datos.html.*
• "El ABC del Derecho de la Unión Europea". EU *Bookshop.*	*http://bookshop.europa.eu/es/el-abc-del-derecho-de-la-uni-n-europea-pbOA8107147/.*
• Propuesta de Reglamento Europeo de Protección de Datos, texto de la Comisión.	*http://eur-lex.europa.eu/legal-content/ES/AUTO/?uri=COM:2012:0011:FIN.*
• Documento de Trabajo de los Servicios de la Comisión. Resumen de la Evaluación de Impacto. SEC/2012/073 final.	*http://eur-lex.europa.eu/legal-content/ES/AUTO/?uri=CELEX:52012SC0073*
• DOUE C 192, 30 de junio de 2012.	*http://eur-lex.europa.eu/legal-content/ES/AUTO/?uri=OJ:C:2012:192:TOC*
• DOUE C 391, 18 de diciembre de 2012.	[1] *Disponible en: http://eur-lex.europa.eu/legal-content/ES/AUTO/?uri=OJ:C:2012:391:TOC*
• Comunicado de Prensa. Consejo de la Unión Europea. 6 y 7 de Diciembre de 2012.	*http://europa.eu/rapid/pressReleasesAction.do?reference=PRES/12/509&format=HTML&aged=0&lg=es&guiLanguage=es.*
• Reglamento Europeo de Protección de Datos, texto del Parlamento Europeo, de 12 de marzo de 2014.	*http://www.europarl.europa.eu/omk/sipade2?PUBREF=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//es.*
• Comisión Europea - Comunicado de prensa. Apoyo de los ministros de Justicia a la propuesta de la Comisión de fijar nuevas normas de protección de datos para impulsar el mercado único digital de la UE.	*http://europa.eu/rapid/pressReleasesAction.do?reference=IP/15/5176&format=HTML&aged=0&lg=es&guiLanguage=es*

- Cuadro comparativo de los tres textos de propuesta de Reglamento General de Protección de Datos. 8 de julio de 2005. *http://data.consilium.europa.eu/doc/document/ST-10391-2015-INIT/en/pdf.*
- Registro de transparencia del Parlamento y la Comisión Europea. Inscripción. *http://ec.europa.eu/transparencyregister/public/staticPage/displayStaticPage.do?locale=es&reference=WHOS_IS_EXPECTED_TO_REGISTER*
- Consejo de Europa. Protección de Datos. Documentos e informes. *http://www.coe.int/t/dghl/standardsetting/dataprotection/docrep_en.asp.*
- Compilación de textos legales del Consejo de Europa sobre protección de datos. *http://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp*.
- *Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (T-PD). T-PD's Rules of Procedure. 1 September 2014.* *http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2014)Rules_Internal_rules%20of%20T-PD_En_Sept_2014.pdf*
- Informe Anual 2014. Agencia Europea para los Derechos Fundamentales. *http://fra.europa.eu/sites/default/files/fra-annual-report-2014_en.pdf.*
- Unión Europea. Declaración de Misión del Comité de las Regiones. 21 de abril de 2009. *http://cor.europa.eu/en/about/Documents/Mission%20statement/ES.pdf.*
- Comité Económico y Social Europeo (CESE) *http://europa.eu/about-eu/institutions-bodies/eesc/index_es.htm*
- CESE. Informe sobre el nuevo Reglamento General de Protección de Datos. *https://dm.eesc.europa.eu/eescdocumentsearch/Pages/opinionsresults.aspx?k=data%20protection*
- Web de la Autoridad de Control en protección de datos alemana. Informes de *Berliner Beauftragter für Datenschutz und Informationsfreiheit*. *http://www.datenschutz-berlin.de.*
- Sobre el GT 29. *http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.*
- *Sixteenth Report of the Article 29 Working Party on Data Protection. European Commission*. 2015. *http://ec.europa.eu/justice/data-protection/article-29/documentation/annual-report/index_en.htm*

- Reglas de procedimiento del GT29. *http://ec.europa.eu/justice/data-protection/article-29/files/rules-art-29_en.pdf.*
- Documentos de trabajo del GT29. *http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm*
- *Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing. GT29. 22 September 2015*. *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf*
- *Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones. GT29. 16 June 2015.* *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf*
- *Explanatory Document on the Processor Binding Corporate Rules. GT29. 22 May 2015.* *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp204.rev_en.pdf*
- *Joint Statement of the European Data Protection Authorities Assembled in the Article 29 Working Party. 26 November 2014.* *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp227_en.pdf*
- *Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12. GT29. 26 November 2014.* *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf*
- *Opinion 8/2014 on the on Recent Developments on the Internet of Things. GT29. 16 September 2014.* *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf*
- Comisión Europea. Supervisor Europeo de Protección de Datos. Publicación de un anuncio de puesto vacante de Supervisor Europeo de Protección de Datos y de Supervisor Adjunto. 2013. *https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/MembersMission/Members/13-07-31_vacancies_ES.pdf.*
- *Compilation Document on Senior Officials Policy. European Commission.* *http://ec.europa.eu/civil_service/docs/official_policy_en.pdf.*

• Decisión del Parlamento Europeo y del Consejo de 4 de diciembre de 2014 por la que se nombra al Supervisor Europeo de Protección de Datos y al Supervisor Adjunto.	*https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/MembersMission/Members/14-12-04_appointingdec_ES.pdf.*
• Sitio del Supervisor Europeo de Protección de Datos.	*https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS*
• Documento para los DPO sobre los Estándares Profesionales de los DPO de las instituciones y organismos de la Unión Europea bajo el Reglamento 45/2001.	*http://ec.europa.eu/dataprotectionofficer/docs/dpo_standards_en.pdf.*
• Documento acerca del rol del DPO en cumplimiento del artículo 24 del Reglamento 45/2001.	*https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PositionP/05-11-28_DPO_paper_EN.pdf.*
• *Monitoring compliance of EU institutions and bodies with Article 24 of Regulation (EC) 45/200. Report on the Status of Data Protection Officers. (EDPS). 17 December 2012.*	*https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Inquiries/2012/2012-12-17_DPO_Status_web_EN.pdf.*
• *Guidelines on the processing of personal data with regard to the management of conflicts of interest in EU institutions and bodies. (EDPS). 8 December 2014.*	*https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/14-12-08_CoI_Guidelines_EN.pdf*
• *Guidelines on the Rights of Individuals with regard to the Processing of Personal Data. (EDPS).*	*https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/14-02-25_GL_DS_rights_EN.pdf*
• *Guidelines on the processing of personal data in the context of public procurement, grants as well as selection and use of external experts. (EDPS).*	*https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/13-06-25_Procurement_EN.pdf*
• *Implementing rules concerning the tasks, duties and powers of the Data Protection Officer (Article 24.8) (EDPS).*	*https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-07-29_Guidelines_DPO_tasks_EN.pdf*

- *Guidelines concerning the processing of health data in the workplace by Community institutions and bodies. (EDPS).* — *https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/09-09-28_Guidelines_Healthdata_atwork_EN.pdf*
- Comentarios sobre Estrategia de Red de Agencias de Medicamentos de la UE para 2020. (EDPS). — *https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2015/15-06-19_EUMA_Network_Strategy_EN.pdf*
- Opinión 1/2015 sobre sanidad móvil. (EDPS). — *https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-05-21_Mhealth_EN.pdf*
- *EDPS Pleading before the Court of Justice. Case C-362/14, Schrems v Data Protection Commissioner. 24 March 2015.* — *https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2015/15-03-24_EDPS_Pleading_Schrems_vs_Data_Commissioner_EN.pdf*
- *EDPS pleading Commission v Hungary (C-288/12) Court of Justice of the EU - 15 October 2013.* — *https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2013/13-10-15_Pleading_EC-Hungary_EN.pdf*
- *Annex to Opinion 3/2015: Comparative table of GDPR texts with EDPS recommendations. (EDPS).* — *https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_Annex_EN.pdf*
- *Opinion 3/2015 (with addendum) Europe's big opportunity. EDPS recommendations on the EU's options for data protection reform. (EDPS).* — [1] *Addenda.- https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-10-09_GDPR_with_addendum_EN.pdf*
- Dictamen 3/2015. La gran oportunidad de Europa. Recomendaciones del SEPD sobre las opciones de la UE en cuanto a la reforma de la protección de datos. (SEPD) — *https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_ES.pdf*
- *EDPS Organisation Chart. Update on 1 November 2015.* — *https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/HR/EDPS_organigram_EN.pdf*

- Sentencia del Tribunal de Justicia de la UE (Gran Sala) de 9 de marzo de 2010. Asunto C‑518/07, — *http://curia.europa.eu/juris/document/document.jsf?text=&docid=79752&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=285506*

- Sentencia del Tribunal de Justicia de la UE (Gran Sala) de 8 de abril de 2014. Asunto C‑288/12. — *http://curia.europa.eu/juris/document/document.jsf?text=&docid=150641&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=285061*

- *European Union Agency for Fundamental Rights (FRA) report. "Access to data protection remedies in EU Member States."* — *http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en.pdf*

- *Report on the data protection perspective of the processing of data on victims of trafficking in human beings. Europol Joint Supervisory Body (JSB). 12 October 2015.* — *http://www.europoljsb.europa.eu/media/277384/on%2012%20october%202015.pdf*

- *Report on the Europol's implementation of the TFTP agreement. Europol Joint Supervisory Body (JSB). May 2015*. — *http://www.europoljsb.europa.eu/media/276578/report%20on%20the%20europol.pdf*

- *Europol Joint Supervisory Body. Data Protection Inspection Report. September 2014*. — *http://www.europoljsb.europa.eu/media/267640/14-41%20final%20data%20inspection%20report%20september%202014-%20v07.pdf*

- Propuesta de Reglamento del Parlamento Europeo y del Consejo. — *http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0173_/com_com(2013)0173_es.pdf*

- Informe de la Autoridad Común de Control de la Europol sobre el nuevo Reglamento del Parlamento Europeo y del Consejo sobre la Agencia de la Unión Europea para la cooperación y la formación en funciones coercitivas (Europol)". — *http://www.europoljsb.europa.eu/media/266424/op%2014-39%20third%20jsb%20op.%20for%20ep%20&%20council%20reg.%20on%20europol.es.pdf*

• Funciones de la Autoridad Común de Control de Eurojust.	*http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/jsb/jsb/The%20Role%20of%20the%20Joint%20Supervisory%20Body%20of%20Eurojust%20(leaflet)/Role-of-JSB-ES.pdf*
• Convenio establecido sobre la base del artículo K.3 del Tratado de la Unión Europea, relativo a la utilización de la tecnología de la información a efectos aduaneros, hecho en Bruselas el 26 de julio de 1995.	*http://www.boe.es/diario_boe/txt.php?id=BOE-A-2000-20182*
• Carta del GT29 al Comisionado de Justicia, Consumidores e Igualdad de Género de la Comisión Europea.17 de junio de 2015.	*http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_letter_from_the_art29_wp_on_trilogue_to_msjourova_en.pdf*
• *European Central Bank. Supervisory Board*.	*https://www.bankingsupervision.europa.eu/organisation/whoiswho/supervisoryboard/html/index.en.html*
• *Caselaw: United States Supreme Court. BOYD v. U S, (1886) February 1, 1886*.	*http://caselaw.findlaw.com/us-supreme-court/116/616.html*
• *The Right to Privacy. Samuel D. Warren and Louis D. Brandeis. Harvard Law Review.*	*http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf*
• *William L. Prosser, Privacy*.	*http://scholarship.law.berkeley.edu/californialawreview/vol48/iss3/1*
• Configuración jurídica del derecho a la privacidad II: concepto y delimitación. *Corral Talciani*.	*http://dialnet.unirioja.es/servlet/articulo?codigo=2650218*
• *Alan F. Westin, Privacy And Freedom*.	*http://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20/*
• *Privacy and Democracy in Cyberspace. Paul M. Schwartz*.	*http://ssrn.com/abstract=205449*

- *Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015. USA government*. *https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf*
- *Records maintained on individuals. US Government information.* *http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf*
- *United States Department of Justice. Overview of the Privacy Act Of 1974. 2015 Edition*. *http://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition*
- *Fair Credir Reporting Act. 15 U.S.C. § 1681 et seq . September 2012*. *http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf*
- *The Report of The Privacy Protection Study Commission. July 1977*. *https://www.ncjrs.gov/pdffiles1/Digitization/49602NCJRS.pdf*
- *Public law 106–102—Nov. 12, 1999. Gramm–Leach–Bliley Act.* *http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf*
- *Electronic Code of Federal Regulations. Title 16: Commercial Practices. Part 312—Children's Online Privacy Protection Rule.* *http://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5*
- *Electronic Code of Federal Regulations. Title 16: Commercial Practices. Part 316—Can-spam Rule.* *http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=cea8be427690a26231dda41b8ccb5f75&ty=HTML&h=L&n=16y1.0.1.3.40&r=PART*
- *"Do-Not-Call Implementation Act" Public Law 108–10—Mar. 11, 2003*. *http://library.clerk.house.gov/reference-files/PPL_108_010_DoNotCallImplementation.pdf.*
- *Agreement on mutual legal assistance between the European Union and the United States of America. 25/06/2003*. *http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?redirect=true&treatyId=5441*
- *European Commission - Fact Sheet. Questions and Answers on the EU-US data protection "Umbrella agreement"*. *http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm*

- *2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.)* — *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML*
- Sitio de gobierno de EEUU para ayuda a las exportaciones. *Swiss Safe Harbor Frameworks.* — *http://www.export.gov/safeharbor/*
- *Memorandum of understanding between the United States Federal Trade Commission and the Office of the Data Protection Commissioner of Ireland on mutual assistance in the enforcement of laws protecting personal information in the private sector.* — *https://www.dataprotection.ie/documents/MOU/MOU.pdf*
- Artículo *"Germany: Pressure increases on Safe Harbor Framework". Data Guidance. 2015 Cecile Park Publishing Ltd.* — *http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=3201*
- Documento de Trabajo 1 sobre los programas de vigilancia de los Estados Unidos y la UE, y su repercusión sobre los derechos fundamentales de los ciudadanos europeos Comisión LIBE. — *http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-524.799&format=PDF&language=ES&secondRef=01*
- Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE. COM(2013) 847 final. — *http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0847_/com_com(2013)0847_es.pdf*
- Sitio de "*Europe v Facebook*". Objetivos de "*europe-v-facebook*". — *http://www.europe-v-facebook.org/ES/Objetivos/objetivos.html*
- *Complaint against Facebook Ireland Ltd – 23 "PRISM". June 25th 2013.* — *http://www.europe-v-facebook.org/prism/facebook.pdf*

- Petición de decisión prejudicial planteada por la *High Court of Ireland* (Irlanda) el 25 de julio de 2014 — *Maximillian Schrems / Data Protection Commissioner*. (Asunto C-362/14). *http://curia.europa.eu/juris/document/document.jsf?docid=157862&doclang=ES*

- Sentencia del Tribunal de Justicia de la UE (Gran Sala) de 6 de octubre de 2015. Asunto C‑362/14, *Maximillian Schrems* y *Data Protection Commissioner*. *http://curia.europa.eu/juris/document/document.jsf;?docid=169195&doclang=ES*

- *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows" and on the Communication from the Commission to the European Parliament and the Council on "the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU.* *https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-02-20_EU_US_rebuliding_trust_EN.pdf*

- Modelo de cláusulas contractuales de la Agencia Española de Protección de Datos para las transferencias internacionales de datos entre encargado y subencargado del tratamiento. *https://www.agpd.es/portalwebAGPD/resoluciones/autorizacion_transf/common/pdfs/MODELO-DEFINITIVO-AEPD_Contrato-encargado-subencargado-21-03-2012.pdf*

- *Statement of the Article 29 Working Party. 16 October 2015*. *http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf*

- *Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems).* COM(2015) 566 final. *http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf*

- Gaceta de Madrid. 19 de febrero de 1900. *https://www.boe.es/datos/pdfs/BOE//1900/050/A00607-00607.pdf*

• Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.	*http://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-12352*
• Real Decreto 2373/1978, de 29 de septiembre, por el que se crea la Comisión Interministerial para la elaboración del Plan Informático Nacional.	*https://www.boe.es/boe/dias/1978/10/07/pdfs/A23348-23349.pdf*
• Orden de 18 de febrero de 1970 por la que se anuncia la celebración de unas "Jornadas de estudio sobre perfeccionamiento y modernización de los medios y métodos de la Justicia", y se convoca a los funcionarios que han de asistir a ellas.	*https://www.boe.es/boe/dias/1970/02/27/pdfs/A03158-03158.pdf*
• Orden de 9 de abril de 1970 por la que se dictan las normas provisionales para la utilización del sistema del "Telex Judicial".	*http://www.boe.es/boe/dias/1970/04/24/pdfs/A06454-06457.pdf*
• Decreto 2880/1970, de 12 de septiembre, por el que se crean la Comisión Interministerial de Informática y el Servicio Central de Informática.	*https://www.boe.es/boe/dias/1970/10/10/pdfs/A16662-16663.pdf*
• Constitución de Portugal de 2 de Abril de 1976.	*http://www.wipo.int/wipolex/es/text.jsp?file_id=179476*
• Sentencia 254/1993, de 20 de julio de 1993. Tribunal Constitucional.	*http://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/2383*
• Sentencia 290/2000, de 30 de noviembre de 2000. Tribunal Constitucional.	*http://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/4274*
• *The Credit Information Act.*	*http://www.datainspektionen.se/in-english/legislation/the-credit-information-act/*
• *The Personal Data Act (1998:204).*	*http://www.datainspektionen.se/in-english/legislation/the-personal-data-act/*
• *Federal Data Protection Act. Language Service of the Federal Ministry of the Interior.*	*http://www.gesetze-im-internet.de/englisch_bdsg/index.html*

• *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*	*http://www.cnil.fr/index.php?id=45*
• *Lov om behandling av personopplysninger (personopplysningsloven).*	*https://lovdata.no/dokument/NL/lov/2000-04-14-31*
• Sentencia 292/2000, de 30 de noviembre de 2000. Tribunal Constitucional.	*http://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/4276.*
• Sinopsis artículo 149 Constitución Española.	*http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=149&tipo=2*
• Ley Orgánica 5/1992. de 29 de octubre. de regulación del tratamiento automatizado de los datos de carácter personal.	*https://www.boe.es/boe/dias/1992/10/31/pdfs/A37037-37045.pdf*
• Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.	*https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750*
• 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.	*https://www.boe.es/buscar/doc.php?id=BOE-A-2008-979*
• Resumen. Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. 2002.	*http://www.oecd.org/sti/ieconomy/15590267.pdf.*
• Resolución 45/95 de Naciones Unidas	*http://www.un.org/es/comun/docs/?symbol=%20A/RES/45/95&Lang=S*
• Agencia Española de Protección de Datos. Marco normativo y régimen jurídico.	*http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/marco-ides-idphp.php*
• Agencia Española de Protección de Datos. Resoluciones y documentos.	*http://www.agpd.es/portalwebAGPD/canaldocumentacion/criterios_art_15/index-ides-idphp.php*

- Sistema universitario andaluz. Consejería de Economía y Conocimiento. Junta de Andalucía. *http://www.juntadeandalucia.es/organismos/economiayconocimiento/areas/universidad/sistema-universitario.html*

- Informe de Reforma de las Administraciones Públicas. Comisión para la Reforma de las Administraciones Públicas. Gobierno de España. *http://www.seap.minhap.gob.es/dms/es/web/areas/reforma_aapp/INFORME-LIBRO/INFORME%20LIBRO.PDF*

- Análisis del Informe sobre la reforma de las Administraciones Públicas elaborado por la Comisión para la Reforma de las Administraciones públicas (CORA). *Autoritat Catalana de Protecció de Datos*. *http://governacio.gencat.cat/web/.content/autogovern/documents/CORA/posicio_acpd_es.pdf*

- Un análisis de la estructura institucional de protección de datos en España. Eduardo López Román. *Universitat* de Barcelona y Juan S. Mora. Banco de España-Eurosistema. 2009. *http://www.indret.com/pdf/641_es.pdf*

- Sitio del *Information Commissioner`s Office* (ICO). *https://ico.org.uk/*

- Órgano de Transparencia y protección de datos de México. *http://inicio.inai.org.mx/SitePages/ifai.aspx*

- Comisión Andaluza de Valoración de Documentos. Consejería de Cultura. Junta de Andalucía. *http://www.juntadeandalucia.es/culturaydeporte/web/areas/archivos/sites/consejeria/areas/archivos/cavad*

- Presupuesto de la Comunidad Autónoma de Andalucía. 2015. *http://www.juntadeandalucia.es/economiayhacienda/planif_presup/presupuesto2015/estado/programas/tomo1_2.pdf*

- Consejo de Transparencia y Protección de Datos de Andalucía. Presupuesto de la Comunidad Autónoma de Andalucía. 2015. *http://www.juntadeandalucia.es/haciendayadministracionpublica/planif_presup/proy_presupuesto2016/estado/servicios/servicios-b-7.pdf*

8 Bibliografía.

ALONSO GARCÍA, R y SARMIENTO, D, *La Carta de Derechos Fundamentales de la Unión Europea,* Aranzadi, Cizur Menor, Navarra, 2006.

AREITIO BERTOLÍN, J**.** *Protección de la seguridad y privacidad en la internet de los objetos (IoT) y su correlación con RFID*. Eurofach electrónica: actualidad y tecnología de la industria electrónica, núm. 386, 2010, p. 42-47.

ARENAS RAMIRO, M. *El derecho fundamental a la protección de datos personales en Europa,* Tirant lo Blanch, Valencia, 2006, p. 225-249.

ARENAS RAMIRO, M. *La Protección de datos personales en los países de la Unión Europea,* Revista Jurídica de Castilla y León núm. 16, 2008, p. 113- 163.

AREY, P. *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press, 2009.

ARNOLD, R."Los derechos fundamentales comunitarios y los derechos fundamentales en las Constituciones nacionales", en MATIA PORTILLA, F.J. (dir.), *La protección de los derechos fundamentales en la Unión Europea*, Cívitas, Madrid, 2002, p. 51-59;

BALAGUER CALLEJÓN, F., "Derecho y derechos en la Unión Europea", en CORCUERA ATIENZA, J. (coord.), *La protección de los derechos fundamentales en la Unión Europea*, Dykinson, Madrid, 2002, p. 39-59.

BARRATI ESTEVE, J. *Dimensión constitucional de la limitación del uso de la informática. La protección de los datos personales*, León, 1997.

BAYO DELGADO, J. "Setting up a new European Authority", en HIELKE HIJMANS AND HERKE KRANENBORG (Eds) *Data Protection Anno 2014: How to restore Trust?,* Cambridge. Intersentia, 2014, p 45-48.

BIGLINO CAMPOS, P. *Derechos fundamentales y competencias de la Unión. El argumento de Hamilton,* Revista Derecho Comunitario Europeo. Año 7, núm. 14, enero-abril 2003.

BLAS, F. *Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales*. Derecho del Estado. Núm. 23, 2009, p. 37-66.

BLOUSTEIN, E.J. *Privacy as an aspect of human dignity: an answer to Dear Prosser*. New York University Law Rewiew vol. 39, 1964, p. 964-1007.

CAREY, P. *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press, 2009.

CARRILLO, M. "La Unión Europea ante los derechos fundamentales", en VV.AA., *La democracia constitucional*. Homenaje al Profesor Francisco Rubio Llorente, vol. II, Centro de Estudios Políticos y Constitucionales, Madrid, 2002, p. 1407-1422.

CERVERA NAVAS, L. Conversaciones. Head of Human Resources and Administration en el Supervisor Europeo de Protección de Datos. Bruselas 15 de septiembre de 2015.

CERVERA NAVAS, L. *El modelo europeo de protección de datos de carácter personal.* Cuadernos de Derecho Público 1997-2007, números 19-20. Instituto Nacional de Administración Pública, p. 131-143.

CORCUERA ATIENZA, J. "La protección de los derechos fundamentales en la Unión Europea: el final de un túnel", en CORCUERA ATIENZA, J. (coord.), *La protección de los Derechos Fundamentales en la Unión Europea,* Dykinson, Madrid, 2002, p. 61-99.

CORRAL TALCIANI, H. *Configuración jurídica del derecho a la privacidad II: concepto y delimitación.* Revista chilena de derecho, vol. 27 núm. 2, Sección Estudios. 2000, p. 331-355.

CREMADES J, y GONZÁLEZ MONTES, J.L. *La nueva ley de internet*, La Ley, Madrid, 2003.

CREMADES, J. y RODRÍGUEZ ARANA, J. (Dirs.), *Comentarios a la Ley General de Telecomunicaciones (aprobada por Ley 32/2003, de 3 de noviembre),* La Ley, Madrid, 2004.

CRUCES BLANCO, E. *El ojo que todo lo ve, el control cibernético de la privacidad: Las ventanas y puertas de la intimidad están abiertas*. Boletín ACAL núm. 89, 2013, p. 5-11.

CRUCES BLANCO, E. *Los portales de la transparencia: Derecho a la información, transparencia y toma de decisiones, ¿leyes transparentes o translúcidas?* Boletín ACAL, núm. 95, 2015, p. 5-7.

CRUCES BLANCO, E. *El acceso a la información, a la documentación y a los archivos. Acceso y gestión documental en la Ley 7/2011, de 3 de noviembre, de Documentos, Archivos y Patrimonio Documental de Andalucía*. Revista TRIA, núm. 17, 2011, p. 143-172.

DAVARA RODRÍGUEZ, M.A. *La protección de datos en Europa. Principios, derechos y procedimientos,* Universidad Pontificia Comillas, Madrid 1998.

DÁVARA RODRÍGUEZ, M. A. *La Ley española de protección de datos (LORTAD): ¿una limitación del uso de la informática para garantizar la intimidad?,* AJA, núm. 76/77, 1992, p.3

DELGADO, L. *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L., 2008.

DESGENS-PASANAU, G., *La protection des données à caractère personnel*, París, LexisNexis, 2012.

DREWER, D. y ELLERMANN, J., *Europol's data protection framework as an asset in the fight against cybercrime,* Foro ERA, Vol. 13, núm. 3, 2013, p. 381–395.

FERNÁNDEZ GARCÍA, *Historia de los Derechos Fundamentales*, en VV.AA. Tomo II Siglo XVIII. Ed. Dykinson (2001), p.26.

FERNANDO PABLO, M.M. *Sobre i-administración*: el Derecho administrativo de la sociedad del conocimiento (I). E-Derecho Administrativo (e-DeA) núm.9, 2003.

FONSECA MORILLO, F.J., "La gestación y el contenido de la Carta de Niza", en MATIA PORTILLA, F.J. (dir.), *La protección de los derechos fundamentales en la Unión Europea*, Civitas, Madrid, 2002, p. 87-121.

FRA (*European Union Agency for Fundamental Rights*) *Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxemburgo, Oficina de Publicaciones de la Unión Europea, 2010.

FREIXES SANJUÁN, T. *Derechos fundamentales en la Unión Europea. Evolución y prospectiva: la construcción de un espacio jurídico europeo de derechos fundamentales*. Revista de Derecho Constitucional Europeo núm. 4, 2005, p. 43-86.

FREIXES SANJUÁN, T. y REMOTTI, J.C., *El futuro de Europa. Constitución y derechos fundamentales*, Minim Ediciones, Valencia, 2002, p. 12-16.

GALÁN JUÁREZ, M. *La interpretación de los derechos fundamentales por parte del Tribunal Constitucional: una argumentación en términos de razonabilidad*, Isegoría, 2006.

GARCÍA-BERRIO HERNÁNDEZ, T. *Informática y libertades. La protección de datos personales y su regulación en Francia y España*. Ed. Universidad de Murcia, 2003, p. 61-62.

GARRIDO FALLA, F. y otros: *Comentarios a la Constitución*, Madrid, 1980, pp. 1813 y ss.

GARRIDO FALLA, F. *El Desarrollo legislativo de las normas básicas y leyes marco estatales por las Comunidades Autónomas*. Revista de Administración Pública núm. 94, enero-abril 1981.

GARRIDO MAYOL, V. *Sinopsis del artículo 149*. Congreso de los Diputados. 2003.

GELMAN, R. "The american approach to privacy supervisión: less than the sum of its parts", en María Verónica Pérez Asinari & Pablo Palazzi (Eds) *Défis su droit à la protection de la vie privée. Challenges of privacy and data protection law*, Bruselas. Bruylant, 2008, p. 611-634.

HAFETZ, JONATHAN L, *"A Man's Home is His Castle?": Reflections on the Home, the Family, and Privacy During the Late Nineteenth and Early Twentieth Centuries*, 8 Wm. & Mary J. Women & L. 175, 2002, p. 175-242.

HEREDERO HIGUERAS, M. *La Agencia de Protección de Datos*, Informática y Derecho núm. 6 y 7, UNED, Mérida, 1994, p. 326.

HERRÁN ORTIZ, I. *El derecho a la intimidad en la nueva ley orgánica de protección de datos.* Dykinson 2002. P. 193.

HERRÁN ORTIZ, I. *La violación de la intimidad en la protección de datos personales*, 1999, p. 344 y 346.

HUSKINX, P. "The Role of Data Protection Authorities", en PÉREZ ASINARI, M.V. & PALAZZI, P. (Eds) *Défis su droit à la protection de la vie privée. Challenges of privacy and data protection law*, Bruselas, Bruylant, 2008, p 561-568.

IBÁÑEZ GARCÍA, I. *Graves ausencias procedimentales en el Derecho administrativo de la Unión Europea*. Instituto de Derecho Europeo e Integración Regional (IEIR) de la Facultad de Derecho de la Universidad Complutense de Madrid, 2014.

JAY, R/HAMILTON, A: *Data protection. Law and practice*, 2ª ed., Sweet & Maxwell, Londres, 2003, p. 518 y 534-536.

KLAUS-DIETER BORCHARDT. *El ABC del Derecho de la Unión Europea*. Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2011.

KUNER, C. *European data protection law*, Oxford, Oxford University Press, 2007.

KUNER, C. *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press, 2013.

LLANEZA GONZÁLEZ, P. *La protección de datos personales en el entorno web*. Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid, núm. 7, 2004.

LOCKE, J. *Segundo Tratado sobre el Gobierno Civil*. Traducción C. Mellizo, Alianza Editorial, Madrid, 1994., núm. 44, p. 70

LÓPEZ-BARAJAS PEREA, M.I. *El deber de conservación de datos en la Unión Europea y sus límites.* Revista de derecho de la Unión Europea, núm. 16, 2009, p. 195-220.

LÓPEZ ROMÁN, E. y MORA, J. *Un análisis de la estructura institucional de protección de datos en España.* INDRET. Revista para el análisis del Derecho, núm. 2. 2009.

LOUVEAUX, SOPHIE. "Ten Years of supervision of the EU Institutions and Bodies", en HIELKE HIJMANS AND HERKE KRANENBORG (Eds) *Data Protection Anno 2014: How to restore Trust?.* Cambridge. Intersentia, 2014, p. 256.

MICHAELIDOU, M. VII Foro de la Privacidad. Ponencia: *Council of Europe data protection standards and the modernization of Convention 108.* Data Privacy Institute, ISMS Forum. Madrid 22.09.2015.

PAVÓN PÉREZ, J.A. *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 de la Universidad de Extremadura nº 19-20. 2001-2002, p. 235 a 252.

PEDROL, X. *La Constitución Europea y sus mitos*, Icaria, Barcelona, 2005.

PÉREZ LUÑO, A. *Informática y libertad. Comentario al artículo 18.4 de la Constitución española*. Revista de Estudios Políticos (Nueva Época), núm. 24, Noviembre-Diciembre 1981, p. 31-53.

PIÑAR MAÑAS, JL. *El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas*, en Cuadernos de Derecho Público, núm. 19-20, 2003, pp. 61-66.

PIÑAR MAÑAS, J.L. "Protección de datos: origen, situación actual y retos de futuro", en *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, p. 84.

PIÑAR MAÑAS, J.L. *¿Existe la privacidad*? Lección magistral en inauguración del Curso Académico 2008-2009. Fundación Universitaria San Pablo-CEU. CEU Ediciones, 2008.

POULLET, Y. & GUTWIRTH, S. "The contribution of the Article 29 Working Party to the construction of a harmonised European data protection system: an illustration of 'reflexive governance'?, en PÉREZ ASINARI, M.V. & PALAZZI, P. (Eds) *Défis su droit à la protection de la vie privée. Challenges of privacy and data protection law*, Bruselas. Bruylant, 2008, p 570-610.

PRISCILA M. REGAN, *Legislating Privacy. Technology, social values and public policy*, Chapel Hill, 1995.

PROSSER, W. *Privacy*, 48 Cal. L. Rev. 383. 1.960.

PUENTE ESCOBAR, A. *La Agencia Española de Protección de Datos como garante del derecho fundamental a la protección de datos de carácter personal*. Azpilcueta. Cuadernos de Derecho, 20. San Sebastián 2008, p. 26.

PULIDO QUECEDO, M. *La catequista y los riesgos de Internet*, en AJA, núm. 602, 2003; y ROSSNAGEL, A. EuGH: Personenbezogene Daten im Internet, en Multimedia und Recht, 2/2004, p. 95-100.

REBOLLO DELGADO, L. *Derechos Fundamentales y Protección de Datos,* Dykinson, Madrid, 2004.

RIPOLL CARULLA, S. "En torno a la calificación de la pasividad española en el cumplimiento del Convenio nº 108 de Europa como acto ilícito internacional", en *La Responsabilidad Internacional*, XIII Jornadas de la AEPDIRI, Alicante 1990, p. 313-330.

ROBLES GARZÓN, J.A. *Nueve estudios para informar un proceso penal europeo y un código modela para potenciar la cooperación jurisdiccional iberoamericana*. Aranzadi, 2013.

RODRÍGUEZ BEREIJO, A. "La Carta de los derechos fundamentales de la Unión Europea y la protección de los derechos humanos", en FERNÁNDEZ SOLA, N. (coord.), *Unión Europea y Derechos fundamentales en perspectiva constitucional*, Dykinson, Madrid, 2004, p. 11-36.

RODRÍGUEZ-VERGARA DÍAZ, A., *Integración europea y derechos fundamentales*, Civitas, Madrid, 2001.

ROSSNAGEL, A. *EuGH: Personenbezogene Daten im Internet*, en Multimedia und Recht, 2, 2004, p. 95-100.

RUBIO LLORENTE, F., "Mostrar los derechos sin destruir la Unión", en GARCÍA DE ENTERRÍA, E. (dir.) y ALONSO GARCÍA, R., *La encrucijada constitucional de la Unión Europea*, Cívitas, Madrid, 2002, pp. 113-150.

RUIZ MIGUEL, C. *El Derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea. Análisis crítico*. Revista de Derecho Comunitario Europeo. Año 7, número 14. Enero-Abril 2003.

SALVADOR MARTÍNEZ, M. Autoridades *independientes*, Ariel, Barcelona, 2002.

SÁNCHEZ BLANCO, A. *Impulso a internet. Perspectiva de los poderes públicos*. Revista del Instituto de Estudios Económicos, núm. 1-2.2001, p.389-414.

SÁNCHEZ BLANCO, A. *La ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos y su significativa proyección sobre el sistema de archivo*. Revista TRIA, núm. 15, 2009, p. 137-160.

SÁNCHEZ BLANCO, A. *Archivos estatales y archivos autonómicos.* Revista Jurídica de Navarra, julio-diciembre 2009, núm. 48, p.131-179.

SÁNCHEZ JIMÉNEZ, E. *Los derechos humanos de la tercera generación: la libertad informática*, en Informática y Derecho, núm. 4, 1994, pp. 165-175.

SANTOS VARA, J. *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, Centro del Derecho de las Relaciones Exteriores, Documento de trabajo del CLEER 2013/2, 2013.

SOUVIRÓN MORENILLA, J.M. "Privacidad y derechos fundamentales", en VVAA, *Introducción a los derechos fundamentales*, vol. III. Ministerio de Justicia, Madrid, 1998, p. 1873-1890.

SCHWARTZ, P.M. *Privacy and Democracy in Cyberspace*, 2.000.

SOUVIRÓN MORENILLA, J.M., "En torno a la jurisdicción del poder informativo del Estado y el control de datos por la Administración". Revista Vasca de Administración Pública, núm. 40, 1994, p. 121-190.

SWIRE, P. "Peter Hustinx and three clichés about EU-U.S. data privacy", en Hielke Hijmans and Herke Kranenborg (Eds) *Data Protection Anno 2014: How to restore Trust?*, Cambridge. Intersentia, 2014, p 191-198.

TÉLLEZ AGUILERA, A. *La protección de datos en la Unión Europea. Divergencias normativas y anhelos unificadores*, Edisofer, Madrid, 2002, p.26-58.

TÉLLEZ AGUILERA, A. *Nuevas tecnologías, intimidad y protección de datos*. Madrid, Edisofer, 2001; p. 211.

TRONCOSO REIGADA, A. *La Distribución competencial entre el Estado y las Comunidades Autónomas en protección de datos personales*. Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas, núm. 1, 2005 (Ejemplar dedicado a: Los derechos fundamentales y las nuevas tecnologías), p. 129.

TRONCOSO REIGADA, A. (dir). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Cívitas, Madrid 2010.

THOMAS ZERDICK . VII Foro de la Privacidad. Data Privacy Institute. Madrid 22 de septiembre de 2015. Ponencia: *European Data Protection Reform*.

WARREN, S.D. y BRANDEIS, L. *The Right to Privacy*. Harvard Law Review, volumen IV, núm. 5, 1890, p. 194-220.

WESTIN, A.F. *Privacy and Freedom*, Washington and Lee Law Review, vol. 25, num. 166. 1968.

WHITE, R. AND OVEY, C. *The European Convention on Human Rights*, Oxford, Oxford University Press, 2010.